Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

OFPPT

ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

DIRECTION RECHERCHE ET INGENIERIE DE FORMATION

SECTEUR TERTIAIRE

RESUME THEORIQUE
&
GUIDE DE TRAVAUX PRATIQUES

Module :
Dépannage de premier niveau d'un réseau local

SECTEUR ***: TERTIAIRE ET NTIC***

SPECIALITE ***: SYSTEME ET RESEAUX INFORMATIQUES***

NIVEAU ***: TECHNICIEN SPECIALISE***

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

REMERCIEMENT

La DRIF remercie les personnes qui ont contribué à l'élaboration du présent document.

Pour la supervision :

- MME.BENNANI WAFAE — DIRECTRICE CDC TERTIAIRE & TIC
- M. ESSABKI NOURDDINE — CHEF DE DIVISION CCFF

Pour la conception :

- BENNANE MOHAMED — Formateur animateur au CDC Tertiaire & TIC

Pour la validation :

- JELLAL ABDELILAH — Formateur animateur au CDC Tertiaire & TIC
- M.BENTALEB ABDELLAH — Formateur animateur au CDC Tertiaire & TIC

Les utilisateurs de ce document sont invités à communiquer à la DRIF toutes les remarques et suggestions afin de les prendre en considération pour l'enrichissement et l'amélioration de ce programme.

Said Slaoui
DRIF

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

SOMMAIRE

	Page
Présentation du module	9
Résumé Théorique	10
I- Notions de base des réseaux locaux	11
- Définition	11
- La carte d'interface	11
- Les médias	11
- Les topologies physiques	12
- Les topologies logiques	14
- Ethernet et Token-Ring	14
- Les systèmes d'exploitation réseaux	15
- Interconnexion des réseaux locaux	16
II- Modèle OSI	18
- Couche physique	19
- Couche liaison	22
- Couche réseau	23
- Couche transport	25
- Couche session	26
- Couche présentation	26
- Couche application	27
Contrôle continu 1	28
III- Protocoles de communication	31
- Définition	31
- Le protocole NETBIOS et NETBEUI	31
- Le protocole TCP/IP	33
IV- Le protocole TCP/IP	36
- Adresse IP	36
- Réseaux et sous-réseaux	38
- Les services d'application utilisant TCP	41
Exercices d'application	45
Contrôle continu 2	48
V- La technologie des serveurs réseaux	50
- Introduction aux serveurs réseaux	50
- Spécificités externes	50
- Spécificités internes	50
- Configuration de base d'un serveur	51
- Mémoire serveur	51
- Ports internes	51
- Processeur serveur	52
- Les technologies multiprocesseurs	53
VI- Préparation du disque dur du serveur	56
- Introduction	56
- Technologie SCSI	56
- Connexion de périphériques SCSI	59
- RAID	59
- RAID Hardware et Software	63
- Solutions RAID Hardware	54
- Partitions de disques	65
VII- Les outils d'administration réseaux et leurs caractéristiques principales	67
- Les spécifications techniques contractuelles	67
- Les solutions d'administration	68
VIII- Analyse des besoins en ce qui a trait à l'installation d'un serveur réseau	77
- La démarche de conception d'un réseau	77

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

IX-	Outils de vérification de l'installation, Commandes TCP/IP	81
	- PING	81
	- IPCONFIG	81
	- NBTSTAT	82
	- NET	82
	- NETSTATISTICS	83
	- NETSTAT	83
	- TRACERT	83
X-	Projet de câblage structuré	85
	- Planification du projet	85
	- Installation des prises de courant et des prises RJ45	89
	- Principes fondamentaux de l'installation des câbles	93
	- Installation des parcours de câbles structurés	97
	- Passage et montage des câbles	100
	- Principes fondamentaux des locaux techniques et des tableaux de conn exion	101
	- Equipements utilisés pour tester les projets de câblage structurés	104
Exercices sur la maintenance du câblage		109
Mini-Projet de conception d'un réseau informatique		111
Contrôle Continu 3		113
XI-	Stratégie de dépannage des réseaux	116
	- Identifier les changements interv enus sur le réseau	116
	- Diviser pour régner	119
	- Le jeu de l'intrus	126
	- Données subjectives, données objectives, analyse et plan	133
	- L'approche naïve	138
XII-	Démarche méthodologique de résolution des problèmes des réseaux locaux	147
	- Méthode scientifique	147
	- Analyse pour le dépannage de réseaux	147
	- Dépannage de réseaux	148
	- Maintenance des ressources partagées	150
Guide des travaux pratiques		151
- At 1 : Principes de base du protocole TCP/IP		152
- At. 2 : Installation et administration de Windows 2000 Server		153
- At 3 : Configuration du client pour les Résea ux MicroSoft dans un domaine		160
- At 4 : Installation Windows 200 Server, configuration initiale		162
- At 5: Les systèmes de fichiers (Windows 2000)		164
- At 6 : Les systèmes de fichiers et poins de montage (Linux)		169
- At 7 : Installation d'une carte réseau		171
- At 8 : Installation de cablâge structuré		172
Evaluation de Fin de Module		175

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

MODULE : Dépannage de premier niveau d'un réseau local

Durée : 191 H
30 % : théorique
70 % pratique

OBJECTIFS OPERATIONNELS DE PREMIER NIVEAU DE COMPORTEMENT

COMPORTEMENT ATTENDU

Pour démontrer sa compétence, le stagiaire doit maîtriser les notions fondamentales relatives aux technologies des réseaux et à Dépanner les dysfonctionnements dans le réseau local
selon les conditions, les critères et les précisions qui suivent.

CONDITIONS D'EVALUATION

- Travaux effectués à partir
  - Etude de cas et de mise en situation (Panne provoquée)
- Travaux effectués à l'aide
  - D'un micro ordinateur (Serveur) et des postes de travail
  - Logiciels réseaux
  - Outils et/ou logiciels de test des réseaux
  - Outils de travail de technicien réseaux

CRITERES GENERAUX DE PERFORMANCE

- Respect de la démarche d'installation d'un réseau local.
- Utilisation judicieuse des sources de référence.
- Utilisation efficace des commandes et des utilitaires du système d'exploitation réseau.
- Respect de la démarche de la résolution d'un problème du réseau local
- Manipulation soigneuse du matériel et des outils de travail

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

OBJECTIFS OPERATIONNELS DE PREMIER NIVEAU
DE COMPORTEMENT

PRECISIONS SUR LE COMPORTEMENT ATTENDU	CRITERES PARTICULIERS DE PERFORMANCE
A. Analyser les besoins en ce qui a trait à l'installation d'un serveur informatique	• Collecte des données appropriées en ce qui concerne les besoins d'installation • d'un serveur informatique : (Système d'exploitation et services) Précision des buts et des fonctions du Serveur • Reconnaissance juste du type de services à installer •
B. Installer un système d'exploitation coté serveur	• Interprétation judicieuse de l'information technique propre aux différents systèmes d'exploitation. • Application correcte de la procédure d'installation appropriée. • Application correcte du paramétrage •
C. Vérifier l'efficacité de l'installation.	• Vérification minutieuse du fonctionnement du système d'exploitation • Résolution efficace des problèmes d'installation relevés.
D. Analyser la demande concernant un problème de dysfonctionnement réseau local	• Interprétation juste de la demande. • Collecte de données complémentaires pertinentes en vue de préciser la nature du problème: - Support de transmission - Connectique - Composants actifs - Client et serveurs...
E. Déterminer les causes et les solutions possibles.	• Etablissement juste des causes possibles. • Choix approprié des outils de diagnostic en fonction du problème. • Utilisation correcte des outils de diagnostic sélectionnés. • Exécution correcte des opérations visant à déterminer la cause principale du problème. • Détermination de différentes solutions appropriées à la résolution du problème.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

PRECISIONS SUR LE COMPORTEMENT ATTENDU	CRITERES PARTICULIERS DE PERFORMANCE
F. Déterminer et appliquer la solution.	• Analyse critique des solutions au regard de la cause principale. • Détermination juste de la solution à appliquer. • Etablissement juste de la séquence des opérations à effectuer. • Application correcte de la solution en fonction des opérations préétablies.
G. Vérifier les résultats et consigner les données l'intervention.	• Inscription juste et complète des détails de l'installation dans la base de connaissance. • Utilisation pertinente de la terminologie Des réseaux locaux

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

OBJECTIFS OPERATIONNELS DE SECOND NIVEAU

LE STAGIAIRE DOIT MAITRISER LES SAVOIRS, SAVOIR -FAIRE, SAVOIR-PERCEVOIR OU SAVOIR-ETRE JUGES PREALABLES AUX APPRENTISSAGES DIRECTEMENT REQUIS POUR L'ATTEINTE DE L'OBJECTIF DE PREMIER NIVEAU, TELS QUE :

Avant d'apprendre à analyser les besoins en ce qui a trait à d'installation d'un serveur informatique (A) :

. Expliquer au stagiaire les notions de base des réseaux locaux
. Définir le modèle OSI et expliquer son interêt
. Présenter la définition d'un protocole de communication
. Présenter le protocole de communication TCP/IP
. Connaître la technologie des serveurs
. Sensibiliser le stagiaire à la préparation correcte des éléments physique du disque dur du serveur;
. Montrer au stagiaire les procédures d'installation fournies dans le manuel d'installation
. Sensibiliser le stagiaire à l'administration des serveurs

Avant d'apprendre Installer un système d'exploitation coté serveur. (B)

9 Expliquer aux stagiaires les étapes d'installation d'un système d'exploitation

Avant d'apprendre à vérifier l'efficacité de l'installation (C) :

10. Sensibiliser le stagiaire à utiliser correctement les outils de vérification de l'installation

Avant d'apprendre à analyser la demande concernant un problème de dysfonctionnement réseau (D) :

11 Montrer au stagiaire la méthode de configuration correctes de la carte réseau.

- é Montrer au stagiaire les étapes de l'installation correcte des systèmes d'exploitation (Client et serveur)
- é Sensibiliser le stagiaire à préparer et installer correctement le système de câblage.
- é Montrer au stagiaire la mise en place correcte des éléments actifs
- é Sensibiliser le stagiaire à la procédure de test

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Avant d'apprendre à déterminer les causes et les solutions Possibles (E)

Sensibiliser le stagiaire à appliquer une démarche méthodique de de résolution des problèmes des réseaux locaux.

Présenter au stagiaire les outils de diagnostic des pannes informatiques

Avant d'apprendre à Vérifier les résultats et consigner les données l'intervention(F):

18.Sensibiliser le stagiaire à utiliser correctement la terminologie en Français et en anglais

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

PRESENTATION DU MODULE

Ce guide de contenu couvre les objectifs d'apprentissage décrits dans le module 8 (***Dépannage de premier niveau d'un réseau local***) de la filière Technicien Spécialisé en Systèmes et Réseaux Informatiques.

Il est divisé en deux parties :
La première partie organisée en douze chapitres, contient un résumé théorique, un ensemble d'exercices d'application, des contrôle continus et des mini-projets. Chacun des chapitre correspondant à un objectif du Guide Pédagogique.
La deuxième partie qui est le guide des travaux pratiques contient …….. ateliers pratiques, chacun contenant les objectifs visés, la durée du TP ainsi que le matériel requis pour le déroulement du TP. Certains de ces ateliers complètent le résumé théorique, d'autres couvrent totalement des objectifs d'ordre pratique

Pour les objectifs 7 (*Montrer aux stagiaire les procédures d'installation fournies dans le manuel d'installation*) et 10 (*Expliquer aux stagiaires les étapes d'installation d'un système d'exploitation*), utiliser la documentation technique du système d'exploitation à installer.
En ce qui est de l'objectif 23 (*Sensibiliser le stagiaire à utiliser correctement la terminologie en français et en anglais*), le stagiaire apprend au fur et à mesure la terminologie des réseaux, le formateur doit donc vérifier l'atteinte de cet objectif tout au long de l'apprentissage du module au cour des évaluation formatives.
Pour le module 24 (*Vérifier les résultats et consigner les données d'intervention*), le formateur doit insister à ce que les stagiaires rendent un rapport ou un compte rendu à la fin de chaque atelier pratique ou mini-projet.

Enfin, une proposition d'examen de fin de module et fournie, le formateur est invité à l'adapter pour mieux évaluer ses stagiaires.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Module : Dépannage de premier niveau d'un réseau local

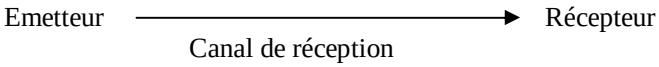
RESUME THEORIQUE

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

I- NOTIONS DE BASE DES RESEAUX LOCAUX

I-1- DEFINITION :

Un réseau est un système de communication reliant plusieurs équipements par des canaux de transmission (câbles, ondes…). Dans le domaine informatique, ces équipements peuvent être d'architecture matérielle et logicielle différente. Le réseau fournit alors, dans la limite possible, des règles nécessaires pour que ces éléments puissent se comprendre.
La communication est un échange d'information entre un émetteur et un récepteur.



Pour qu'il y ait communication, il faut qu'il y ait compréhension, d'où la nécessité d'un code.
Exemple :
Morse (télégramme), langage
Ascii (ordinateur), langage

POURQUOI UN RESEAU ?

. Partage des ressources physiques :
  - Imprimante
  - Lecteur de CD-ROM
  - Disque dur de grande capacité

. Partage des ressources logicielles : Accès de plusieurs utilisateurs à des applications sans avoir à les installer sur leur propre poste.
. Partage des données : Plusieurs utilisateurs peuvent accéder aux mêmes données et peuvent faire des modifications en temps réel.
. Centralisation des sauvegardes : sécurisation contre des risques comme le vol, l'incendie, la suppression…
. Sécurité : on peut affecter à chaque utilisateur des droits sur telle ou telle donnée.
. Accès à un ensemble de services : vente, réservation, banque…
. Publication et diffusion de documents : Internet.
. Communication entre personnes distantes par le son, le texte et l'image : messagerie, conférence, chat…
. Recherche d'informations : Internet
h. Gestion de parc informatique : inventions, licences…

I-2- LA CARTE D'INTERFACE RESEAU (NIC : Network Interface Card) :

La carte réseau est un élément indispensable d'un ordinateur au réseau. Elle a pour rôle de modifier et d'amplifier les signaux numériques pour qu'ils puissent traverser le câble du réseau ; et puisque l'ordinateur est toujours plus rapide que le réseau, la carte réseau constitue une mémoire intermédiaire.

I-3- LES MEDIAS :

Les médias sont les supports physiques de la transmission utilisés dans le réseau. Ils servent à lie r et à mettre en contact l'ensemble des nœuds avec le réseau. On appelle nœud tout point de connexion d'un élément d'émission ou de réception au réseau.
La liaison entre le média et l'ordinateur (le nœud) se fait en général par des connecteurs.

1- Paire torsadée non blindée (UTP : Unshielded Twisted Pair)

§ Description : ce support est constitué de quatre paires de fils conducteurs recouverts d'un isolant et torsadés deux à deux pour mieux résister aux perturbations.
§ Connecteur : RJ45 (le connecteur utilisé dans le réseau téléphonique est RJ11).
§ Transmission : UTP permet la transmission sur de courtes distances.
§ Débit : UTP peut atteindre 100 Mbps, mais elle est surtout utilisée avec 10 Mbps.
§ Bande passante : elle est de 1 à 4 Mhz.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

§ Coût et installation : relativement à d'autres câbles, l'UTP est la moins chère et la plus facile à installer. Son connecteur est petit et il est surtout utilisé quand la transmission va se faire avec un débit faible sur une bande passante étroite et sur une courte distance.

2 - Paire torsadée blindée (STP :Shielded Twisted Pair)

§ Description : ce support est constitué de deux paires torsadées de fils conducteurs recouverts d'un isolant. Chaque paire est enveloppée dans une gaine protectrice. Les deux gaines sont entourées d'un blindage qui permet de mieux résister aux perturbations.
§ Connecteur : hermaphrodite (connecteur IBM)
§ Transmission : la transmission avec le STP est relativement supérieure à la transmission avec l'UTP mais elle reste courte relativement à d'autres supports (i nférieure à un km)
§ Débit : à peu près 10 Mbps (jusqu'à 16 Mbps)
§ Bande passante : 1 à 4 Mhz
§ Coût et installation : la STP coûte assez cher. Elle utilise un gros connecteur et n'est pas très exploitée sur le marché. Son véritable avantage relativement à l'UT P est qu'elle résiste mieux aux perturbations.

3 - Le câble coaxial :

§ description : ce support est constitué de deux conducteurs cylindriques de même axe séparés par un isolant
§ connecteur : BNC(Britsh Naval Connector)
§ transmission : elle est moyenne mais peut être grande en large bande (jusqu'à 10 km)
§ débit : entre 10 et 50 Mbps
§ bande passante : la transmission en bande de base (normale) est entre 1 et 100Mhz. Dans la transmission en large bande, elle est entre 50 et 400 Mhz
§ coût et installation : le prix d'un câble coaxial est moyen, son installation est facile, son connecteur est petit. Mais le rapport qualité prix fait que les entreprises utilisent surtout l'UTP.

4 - la fibre optique : (signal lumineux, passe rapidement)

§ description : elle est constituée de deux fibres en verre entourées chacune d'une gaine. Chaque gaine est entourée de fibres en Kevler (renforcement appelé revêtement qui assure la rigidité du câble).
§ Chaque fibre ne fonctionne que dans un seul sens.
§ Connecteur : ST
§ Transmission : elle se fait sur une très grande distance (80 km au minimum jusqu'à atteindre des centaines)
§ Débit : 500 Mbps minimum
§ Bande passante : elle est de l'ordre de plusieurs Ghz
§ Coût et installation : la fibre optique coûte très cher, elle est très délicate à install er car son installation demande un technicien spécialisé dans le domaine.

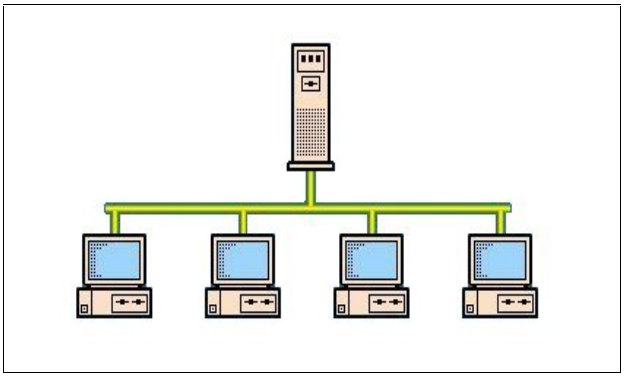
I-4- LES TOPOLOGIES PHYSIQUES :

L'implantation physique d'un réseau, appelée topologie physique, peut se faire de différentes manières :

1 - Topologie en bus :

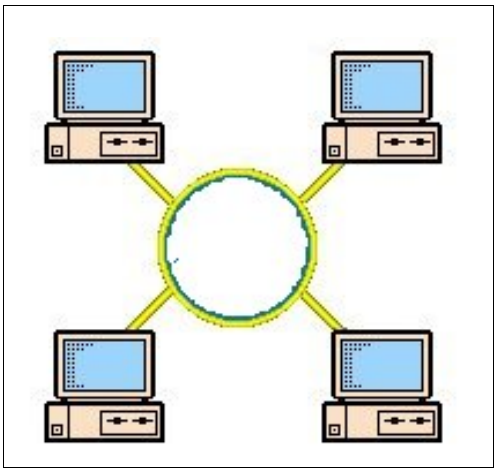
Les différents éléments du réseau sont montés en série. Ce genre de structure nécessite l'utilisation de bouchons de terminaison qui empêchent le signal de rebondir en l'absorbant.
NB : sans bouchon de terminaison, le signal retourne sur le média en créant des parasites.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com



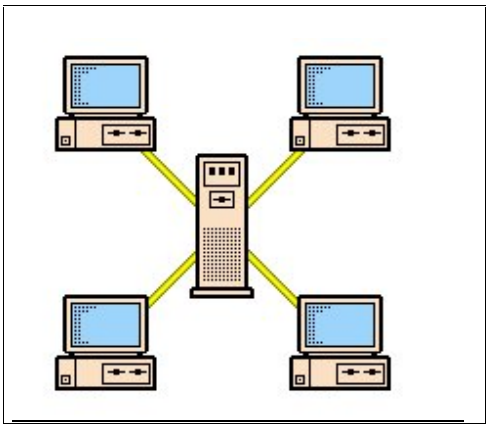
2 - Topologie en anneau :

Les différents éléments du réseau sont montés en série sur une bande fermée.



3 - Topologie en étoile :

Les câbles de connexion vont d'un nœud vers les stations.



4 - Comparaison :

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Topologie	Avantages	Inconvénients
BUS	§ Facile à installer. § Un seul câble pour l'ensemble. § Branchement de nouveaux nœuds sans perturbation du réseau.	§ Difficulté de localisation des pannes. § En cas de rupture, le réseau entier s'arrête.
ANNEAU	§ Un seul câble.	§ Toute panne au niveau d'un élément ou coupure de câble bloque le réseau. § Le temps de réponse se dégrade à l'ajout d'un nouveau nœud.
ETOILE	§ Facilité de localisation des pannes. § Possibilité d'extension : les nœuds s'y ajoutent facilement.	§ Il y'a autant de câbles que d'équipements, cela peut coûter cher pour des nœuds éloignés.

I-5- LES TOPOLOGIES LOGIQUES :

Quand le signal est envoyé, il passe chez tous les récepteurs. Il sera intercepté par le récepteur concerné grâce aux adresses de l'émetteur et du récepteur.
Une méthode d'accès détermine la façon avec laquelle se déroule la communication entre les nœuds du réseau. Elle limite les conflits, elle constitue la trame, elle détermine la façon d'accéder au câble et contrôle cet accès.

1 - CSMA/CD : « Carrier Sense Multiple Access/Collision Detection »
Toute information envoyée par un nœud atteindra tous les autres nœuds du réseau. Chaque nœud a une adresse unique. Il reste constamment en écoute du câble pour détecter les signaux qui passent sur le réseau. Au passage d'un signal, il vérifie si l'adresse destinataire est son adresse. Si c'est le cas, il prend le message et le lit, sinon il le néglige.
« **IRQ** --- interruption : chaque élément de l'ordinateur communique avec le microprocesseur par un numéro d'interruption »
Si un nœud veut émettre, il doit s'assurer qu'il n'y a aucun message sur le câble. Il peut arriver que deux nœuds émettent en même temps, il y aura alors une collision qui sera entendue par l'ensemble des nœuds du réseau. L'émission sera reprise après un temps aléatoire qui, en général, n'est jamais le même. Ce temps aléatoire fait de CSMA/CD une méthode non déterministe.

2 - la méthode d'accès à jeton :
Un jeton = un signal qui circule constamment sur le réseau, de poste en poste.
Lorsqu'une station désire émettre, elle doit attendre de recevoir le jeton dans un état libre. Elle le charge avec les informations, le marque occupé et elle le renvoie sur le réseau à la station suivante. Cette station vérifie le message, trouve que c'est occupé, contrôle si il lui est destiné. Si c'est le cas, elle lit les informations, rajoute une indication qui va informer la station expéditrice que son message a été reçu. Si, par contre, le message ne lui est pas destiné, elle le réécrit et le laisse passer à la station à côté.

Ce travail se refait par chaque station jusqu'à ce que le jeton arrive à la station émettrice qui vérifie si le message a été reçu. Si c'est le cas, elle libère le jeton et le renvoie sur le câble.

I-6- ETHERNET ET TOKEN-RING :

Ethernet → CSMA/CD → IEEE 802.3 ou ISO. 8802.3 (Février 1980)
IBM Token-Ring → Anneau à jeton → IEEE 802.5 ou ISO 8802.5

La méthode **CSMA/CD** a été adoptée par un standard qui s'appelle **ETHERNET** alors que la méthode d'**accès à jeton** a été adoptée par le standard **Token-Ring.**

1 - ETHERNET :

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

La technologie Ethernet fut proposée par XEROX, INTEL, DIGITAL à la normalisation IEEE (Institute of Electrical and Electronic Engineering, société qui s'occupe de la normalisation en électronique) et fut désignée avec quelques modifications IEEE 802.3 (ISO 8802.3)

	IEEE 802.3 10 Base T	**IEEE 802.3 10 base 5**	**IEEE 802.3 10 Base 2**
méthode d'accès	CSMA/CD	CSMA/CD	CSMA/CD
débit	10 Mbps	10 Mbps	10Mbps
câble	paire torsadée non blindée (UTP)	coaxial épais	Coaxial noir (thin Ethernet cheapernet)
connecteur	RJ45	RJ11	BNC
distance max. entre 2 nœuds	100 m	500 m	185 m
topologie physique	Etoile	Bus	Bus
le nombre max. de HUB	4		
transmission	bande de base	accès par Tranceiver	bande de base
utilisateurs		100 maximum	30

Tranceiver : élément de liaison entre connecteur AUI sur une carte réseau et un connecteur en T monté sur un câble coaxial épais.
AUI : connecteur femelle à 15 broches qui peut se trouver sur la carte réseau
Remarque : il existe d'autres normes ETHERNET comme 802.3 Broad 36(large bande) et IEEE 802.3 10 Base F (fibre optique)

Il y a également sur le marché des normes Ethernet à haute vitesse. En effet, les besoins actuels de l'entreprise, le transfert d'image, de séquence vidéo, ont amené un grand développement d'Ethernet qui peut fonctionner aujourd'hui à 100 Mbps. Aussi, plusieurs normes ont vu le jour dans ce sens : le 100 Base TX, 100 Base T4…

2 - TOKEN-RING :

La technologie des réseaux Token-Ring fut développée par IBM. Elle a été normalisée par l'IEEE sous la norme IEEE 802.5. contrairement à Ethernet, il n'existe pas, sur le marché, de normes concernant l'implantation de ce type de réseau. Pour ces raisons, on adopte en général les spécifications IBM. Les types ci-dessous ne sont pas des normes mais des recommandations IBM.

	Type 1	**Type 2**	**Type 3**
méthode d'accès	à jeton	à jeton	à jeton
débit	4 ou 16 Mbps	4 Mbps	4 Mbps
câble	paire torsadée blindée	paire torsadée blindée + une paire de fils	paire torsadée non blindée
connecteur	IBM Hermaphrodite	IBM	RJ45
utilisateurs	260 stations par Anneau		260 stations par Anneau
topologie (avec MSAU)	Etoile	Etoile	Etoile
distance nœud - MSAU	145 m max.	375 m max.	100 m max.
distance MSAU - MSAU	200 m	400 m max.	300 m max.

Remarque : la MSAU transforme une topologie physique Etoile en Anneau.

I-7- LE SYSTEME D'EXPLOITATION RESEAU : (NOS : Network Operating System)

C'est un ensemble de programmes qui donnent à certains ordinateurs et périphériques la capacité d'accepter les requêtes de service en provenance du réseau ou d'émettre des requêtes.
Il est composé de deux parties, une partie **Client** et une partie **Serveur**. La partie Serveur est chargée de la gestion des autorisations, de l'exécution des services requis ou demandés, alors que la partie Client permet au Système d'exploitation d'envoyer au Serveur les requêtes via un redirecteur qui capture les demandes de service externes et les redirigent vers le réseau.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Remarque : la partie Client peut être intégrée sur certains NOS (exemple : Windows 95, Windows 98…), mais doit être installée sur d'autres.

I-8- INTERCONNEXION DES RESEAUX LOCAUX

On assimile très souvent le réseau local au Réseau d'entreprise. Mais pour des raisons organisationnelles ou géographiques, le Réseau d'entreprise peut se di viser en plusieurs réseaux locaux en fonction des services, des étages, des établissements, de l'importance du trafic, de la sécurité…
Un réseau d'entreprise peut également vouloir se connecter à d'autres réseaux d'entreprise. c'est pour cela que l'évolution du réseau local en réseau d'entreprise nécessite l'utilisation d'un ensemble d'équipements d'interconnexion des réseaux.

1 - Le répéteur :

Un signal ne peut pas se propager infiniment sur le câble. Il s'affaiblit jusqu'à s'atténuer complètement. Cette atténuation est fonction du type de câble et c'est d'ailleurs un critère de choix des câbles.
Pour prolonger les réseaux au delà des limites d'un câble, on utilise un **répéteur**.
un répéteur ne fait que régénérer le signal. Il n'est pas responsable de la dét ection des erreurs ou de leur correction. Quand un signal est présent sur un câble, le répéteur l'amplifie et le véhicule sur un autre câble de même type ou de type différent. Il est incapable de modifier la nature de la trame et donc il ne peut pas interconnecter des réseaux hétérogènes (Ethernet et Token -Ring)
Remarque : le nombre de répéteurs à utiliser dépend du standard utilisé (Ethernet ou Token -Ring). Un réseau reste donc limité même avec l'utilisation des répéteurs.

2 - Le pont (gestion du trafic) :

Pour soulager un réseau où les flux sont devenus très importants et donc le temps de réponse trop long, il faut le segmenter et utiliser des ponts.
Un pont permet d'interconnecter deux ou plusieurs segments d'un réseau. Son rôle principal est de filtrer les différentes requêtes et de distinguer les informations destinées à un élément d'un même segment de celles destinées aux éléments d'un autre segment. En fait, chaque nœud est identifié avec une adresse unique. Dans les anciennes générations de ponts, l' administrateur réseau devait introduire manuellement ses adresses pour que les ponts puissent reconnaître les nœuds et leur emplacement dans les segments du réseau.
Les nouvelles générations sont plus intelligentes. Les ponts gardent automatiquement l'adr esse de chaque trame qui transite par le réseau et apprend à localiser le nœud ; ainsi après une étape d'auto apprentissage, il ne laissera passer que les trames destinées à l'autre segment du réseau.
Les ponts contribuent également à étendre les limites d 'un réseau en reliant plusieurs segments du réseau. Ils limitent aussi les problèmes de collision, si une collision a lieu dans un segment, elle ne sera pas filtrée et l'autre segment pourra fonctionner correctement.
Remarque : les ponts ne peuvent pas connecter des réseaux hétérogènes.

3 - Le routeur :

Ces appareils sont utilisés pour trouver le meilleur chemin de communication entre différents réseaux. Ils utilisent une table de routage qui contient les meilleurs chemins à suivre pour chaque nœud du réseau et à partir de tous les nœuds du réseau.

Les routeurs permettent plus d'un chemin et déterminent la meilleure route en fonction de différents critères (rapidité, données). Ils sont très adaptés aux réseaux complexes et gèrent simultanément plusieurs lignes de communication en optimisant l'utilisation de ces lignes et en répartissant les transmissions en fonction des occupations de chaque ligne.

4 - La passerelle :

Ce sont des éléments d'interconnexion pour des réseaux utilisant des protocoles différen ts.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Les passerelles permettent la conversion des protocoles, elles font ce travail en supprimant les couches d'informations des protocoles reçues et en les remplaçant par les couches d'informations requises par les nouveaux environnements.

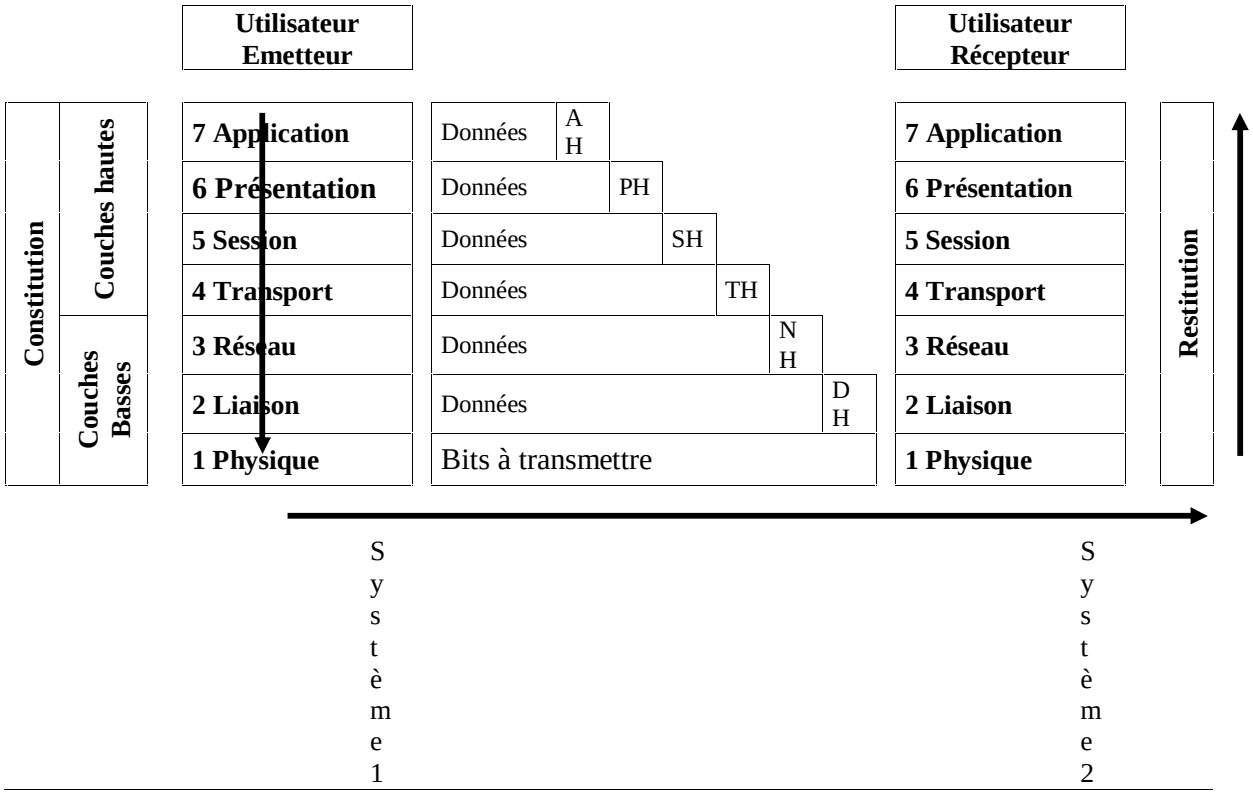
Remarque : les passerelles peuvent être implantées sous forme logicielle ou matérielle.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

II- LE MODELE OSI

Un des soucis majeurs dans le domaine des réseaux est de faire communiquer entre eux des systèmes hétérogènes et d'offrir ainsi à l'utilisateur une plus grande liberté de choix de l'ISO (International Standard Organization).
L'ISO, en collaboration avec l'UIT (Union Internationale de Télécommunications, jadis CCITT) a défini un modèle de référence qui gère les règles des échanges entre deux systèmes qu'on veut interconnecter.
Le modèle se présente en sept couches superposées. Il s'appelle le modèle OSI (Open System Interconnexion).
Ces couches regroupent l'ensemble des fonctionnalités (tâches) requises lors d'une communication réseau.

L'intérêt d'un modèle est de réduire la complexité des communications et d'isoler les différentes fonctions. De cette manière, le changement d'une fonction ne devra pas affecter toute l'architecture.



Les couches basses, qu'on appelle également couches de communication, définissent les fonctions permettant le transfert à travers le réseau de l'information provenant des couches supérieures. Les couches hautes, qu'on appelle également les couches de traitement, comportent les règles de transfert de l'information, de contrôle de flux de dialogue et de présentation.

- Une couche du système 1 ne peut communiquer qu'avec le même couche du système 2. Cette communication ne peut pas se faire directement ; la couche en question **doit demander un service** à la couche inférieure et ainsi de suite.
- Quand les informations vont arriver au système 2, chaque couche va **fournir un service** à sa couche supérieure.
- Les règles d'échange entre 2 couches sont définies dans une interface qui décrira un point d'accès aux services « SAP » (Service Access Point). Un SAP se trouve à la limite entre deux couches et va indiquer à un protocole où il doit adresser sa demande à la couche n-1 (inférieure)
- Une couche transmet tout ce que lui transmet la couche supérieure mais y ajoute ses propres informations (AH,PH…). Quand le message arrive à la couche physique de l'émetteur, elle le

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

transmet à la couche physique du récepteur et l'opération se fait dans le sens inverse. Chaque couche devra enlever ce que la couche qui lui ressemble sur l'autre système a mis et ainsi de suite jusqu'à ce que le message soit restitué.

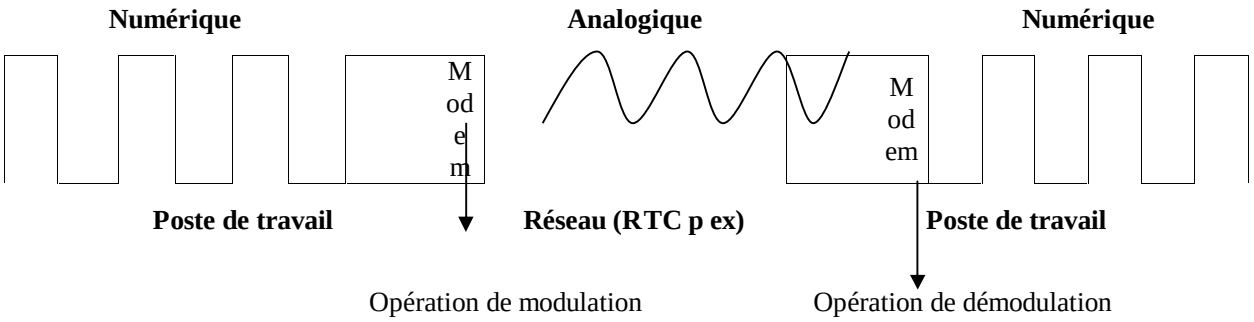
§

II-1- LA COUCHE PHYSIQUE :

Elle comporte tout ce qui concerne l'établissement de la liaison, elle fournit les caractéristiques mécaniques, électriques et fonctionnelles nécessaires à l'initialisation, au maintien et à la désactivation d'une communication. La couche physique s'intéresse alors :

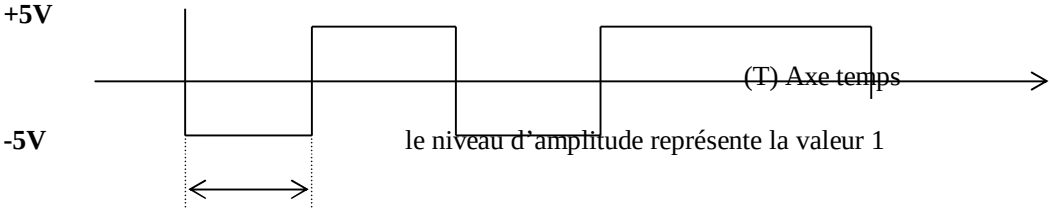
- § Au nombre de volts à atteindre pour représenter un bit à 1 ou à 0.
- § A la durée d'un bit.
- § A la possibilité de transmettre dans les 2 sens (Simplex, Half Duplex ou Full Duplex).
- § Au nombre de broches que doit posséder un connecteur réseau.
- § A l'utilisation de chaque broche.
- § Au support physique de la transmission (câble).
- § Aux normes et avis à utiliser pour assurer ces fonctions.
- § A la nature du signal à transmettre (numérique ou analogique).
- § Aux équipements à utiliser (modem, TNR, Multiplexeur, Répéteur).
- § Au type de modulation à utiliser (Modem).
- § Au choix d'un mode de transmission (Synchrone ou asynchrone).

1 – La modulation :



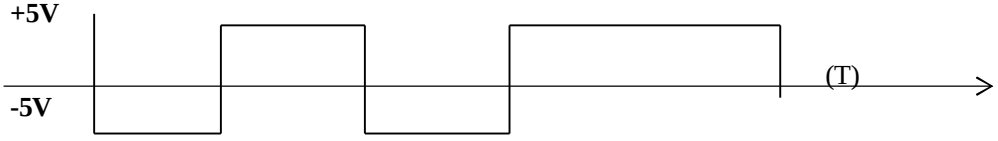
La modulation sert à adapter un signal numérique aux conditions de ligne analogique. Cette opération est possible par l'utilisation d'appareils électroniques appelés Mod ems.
Il existe 3 types de modulation :

§ Modulation d'amplitude

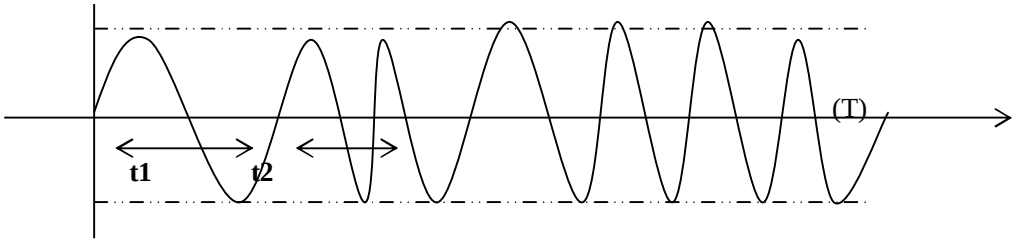


Remarque : le passage de 0 à 1 est indiqué par le niveau d'amplitude.

§ Modulation de fréquence :

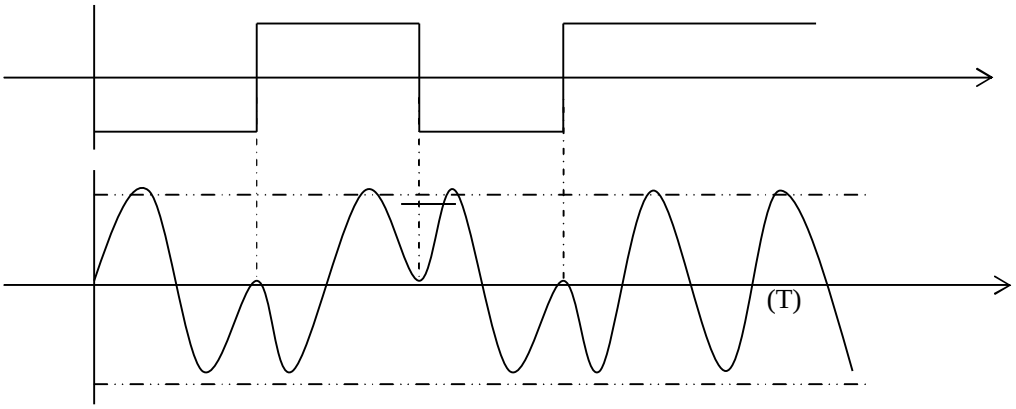


Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com



Remarque : le passage de 0 à 1 est indiqué par le changement de fréquence.
La fréquence N est calculée en Hz
Période T=1/N

§ Modulation de phase :



Remarque : le passage de 0 à 1 est indiqué par le changement de phase.

Le passage du signal numérique au signal analogique se fait selon un principe mathématique assez compliqué représenté par les séries de Fourrier.

2 – La démodulation :
c'est l'opération inverse de la modulation, c'est à dire transformer un signal analogique en signal numérique. C'est également le Modem qui est responsable de cette opération qu'on appelle échantillonnage.

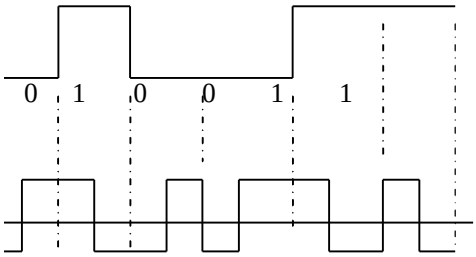
3 – La codification numérique :
il est très difficile de faire passer du courant continu entre deux stations et spécialement il est difficile de faire passer un courant nul pour indiquer un zéro binaire et un courant positif pour indiquer un 1 binaire. Il y a différentes techniques pour représenter numérique en numérique.

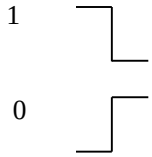
§ ***Code NRZ*** *(No Return to Zero)*
La valeur (0) sera représentée par un signal négatif et la valeur binaire (1) sera représentée par signal positif (son opposé)

§ ***Code NRZI*** *(No Return to Zero Inverse)*
C'est le code NRZ inversé. Valeur binaire 1 : signal négatif – Valeur binaire 0 : signal positif.

§ ***Code Biphase Manchester***
Valeur binaire 1 : transition (passage) de haut en bas au milieu de l'intervalle.
Valeur binaire 0 : transition (passage) de bas en haut au milieu de l'intervalle.

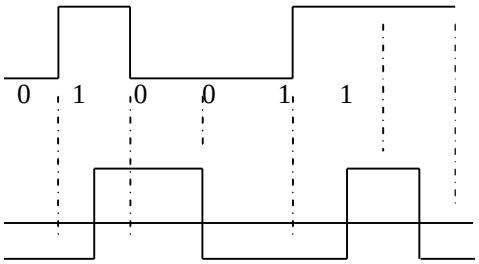
Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com





§ ***Code Miller*** *(Delay Mode)*

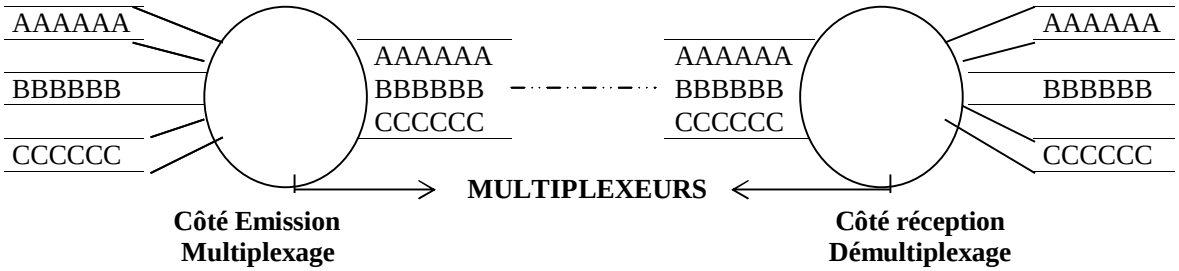
Le code Miller utilise une transition au milieu du bit pour représenter le (1) et n'utilise pas de transition pour représenter la valeur binaire (0). Il utilise un transition à la fin du bit si le bit suivant est (0).



4 – Les multiplexeurs(MUX):

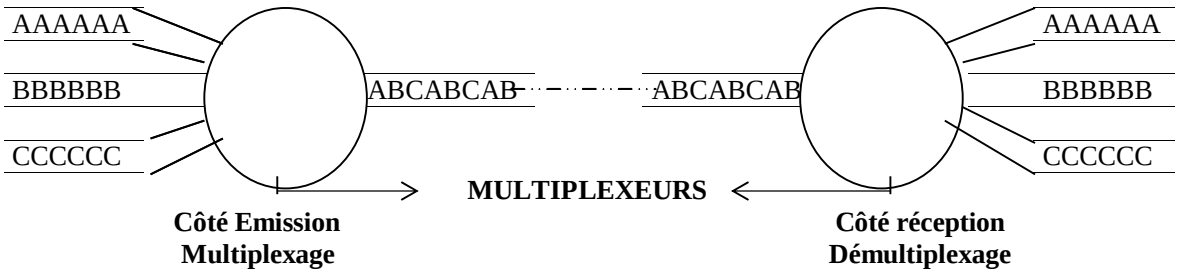
Ce sont des appareils électroniques qui permettent de faire passer plusieurs signaux sur un minimum de canaux. Le multiplexage se fait de 2 manières :

§ **Le multiplexage de fréquence :** (FDM : Frequency Division Multiplexing)



On découpe un canal haut débit en sous canaux ayant chacun une plage de fréquence (Nombre d'oscillations dans un même plage horloge).

§ ***Le multiplexage temporel :*** *(TDM : Time Division Multiplexing)*



Le MUX prélève successivement sur les différents canaux d'entrée des bits pour construire un train de bits à transmettre à la ligne commune.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

II-2- LA COUCHE LIAISON :

L'IEEE décompose la couche liaison en deux sous-couches :

- **LLC** : Logical Link Control
- **MAC** : Media Access Control

La sous-couche MAC est responsable de la constitution des trames quand les données sont en cours d'émission et elle est responsable du découpage du train de bits en trames si les données sont en cours de réception. Au niveau de la MAC, on trouve l'adresse qui permet d'identifier la machine d'une manière unique au niveau mondial (adresse MAC : Manufactured Adress Card). C'est également au niveau de la MAC qu'il est question de méthodes d'accès (CSMA/CD – Anneau à jeton)

La sous-couche LLC s'occupe de tout ce qui est procédures de contrôle et détection d'erreurs.

1 – la sous-couche MAC :

A	B	C	D	E	F
Champ de début de trame	**Champ d'adresse**	**Longueur et type de trame**	**Champ de données**	**Champ des FCS**	**Champ de fin de trame**

ENCAPSULAGE DE LA TRAME (encadrement)

DLE/STX (data link espace / start of text)			Données provenant de la couche réseau	Rôle de la sous-couche LLC	DLE/ETX (data link espace / End of text

- **A** : séquence d'octets prévenant le récepteur du début de la trame
- **B** : adresses des machines source et destination
- **C** : champ indiquant la longueur de la trame
- **D** : Données transmises par la couche réseau (émetteur et récepteur)
- **E** : séquence de détection et de correction d'erreurs
- **F** : séquence d'octets indiquant la fin de la trame.

Si la couche liaison (sous-couche MAC) vient de recevoir les données de la couche physique, elle doit rechercher la séquence de début de trame et la séquence de fin de trame pour l'isoler et pouvoir la traiter. Ensuite, elle doit vérifier si l'adresse de destination correspond à celle du système auquel elle appartient. Si c'est le cas, elle enlève tous les champs de la trame exceptés les champs D et E qu'elle fait passer à la sous-couche LLC.

Si jamais la sous-couche MAC découvre que l'adresse destinataire ne correspond pas à la sienne, elle néglige la trame ou s'occupe de la faire passer à la station suivante (selon la méthode d'accès).

Si les données viennent de chez la sous-couche LLC (de la couche réseau), la sous-couche MAC va prendre ces données, leur ajouter les champs B et C et les encapsuler (les encadrer) par les champs A et F puis les faire passer à la couche physique.

2 – l'adressage MAC :

Pour vérifier si une trame est destinée à la machine, la couche liaison (MAC) compare l'adresse du destinataire se trouvant dans la trame avec l'adresse MAC (ne pas confondre MAC et MAC). L'adresse MAC est une adresse implantée par le fabriquant de la carte réseau dans la ROM de celle-ci. Elle se présente sous la forme de 12 chiffres hexadécimaux.

Remarque : les bases de calcul sont au nombre de 4 :

- **Binaire** : 2 chiffres 0 et 1 ;
- **Octal** : 8 chiffres ;
- **Décimal** : 10 chiffres de 0 à 9 ;

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

§ **Hexadécimal** : 16 chiffres de 0 à 9 + les lettres A, B, C, D, E et F (10 à 15).

3 - la sous-couche LLC :

Toutes les trames peuvent connaître des erreurs lors de la transmission. Les sources de ces erreurs sont variées. Exemples :

§ **Le bruit thermique** : c'est un problème toujours présent. Il est dû à l'agitation des électrons sur les câbles.
§ **Le bruit impulsif** : il résulte d'étincelles de rupture de surtension.
§ **Deux lignes proches** physiquement.
§ **Les liaisons par ondes hertziennes** : elles sont sujettes à l'affaiblissement à cause d'un certain nombre de phénomènes comme le passage d'oiseaux ou d'une moto.

Quand un micro reçoit une trame, il doit reconnaître si elle contient des erreurs : c'est le rôle de la sous-couche LLC. Il existe différentes méthodes pour calculer et détecter les erreurs dans une trame :

§ **Le code de redondance cyclique (CRC)** : il permet de calculer les erreurs en utilisant des polynômes ($f(x)=ax^n + bx^{n+1}$…)
§ **Parité bidirectionnelle** : elle permet de rajouter des bits au message original. Ces bits représentent un nombre pair ou impair de « 1 » binaires
§ **Nombre de caractères** : il permet d'ajouter au message original le nombre total de bits

La sous-couche LLC de l'ordinateur source calcule la séquence de contrôle d'erreurs et l'ajoute au message. La LLC de l'ordinateur cible examine les données reçues, calcule la séquence de contrôle (en utilisant la même méthode que l'émetteur) et vérifie si elle correspond à celle obtenue par l'ordinateur source.

La procédure LLC est définie dans la norme IEEE 802.2 (touche uniquement la couche 2)

II-3- LA COUCHE RESEAU

Elle assure l'acheminement et le routage (choix du meilleur chemin) de l'information à travers le réseau. Elle assure également un rôle de contrôle de flux et d'adressage.
Adressage : la couche réseau utilise en général un système d'adressage spécial. En fait l'adresse MAC correspondante. C'est pour cela que la couche réseau utilise un adressage logique hiérarchique. Parmi les protocoles les plus utilisés on trouve le protocole IP (Internet Protocol). Au niveau de ce protocole, on peut définir des adresses IP qui sont très adaptées aux ad resses hiérarchiques. Une adresse IP se compose de 4 octets séparés par des points. Chaque octet est sur 8 bits.

Exemple : 11000000.00000101.00100010.00001011.
Pour faciliter la manipulation des adresses IP, on les représente sous forme dé cimale. Pour cela, il faut faire des conversions de la base binaire à la base décimale.
Ex : 192.5.34.11

1 - Les classes des adresses IP

Dans une adresse IP, on trouve toujours une partie concernant le réseau et une partie concernant l'adresse de la station (hôte). Cette répartition se fait selon 3 classes A, B et C

- **La classe A** : Les adresses IP de la classe A utilisent les 8 premiers bits pour l'adressage réseau. Les bits restant vont désigner les hôtes. Donc dans la classe A, on peut obtenir jusqu'à 2^{24} adresses dans un même réseau.
  Pour reconnaître une adresse IP de la classe A, on vérifie si le 1^{er} bit du 1^{er} octet de l'adresse IP est un 0, ou bien on vérifie si le 1^{er} nombre décimal de l'adresse est compris entre 0 et 127.
- **La classe B** : Les adresses IP de la classe B utilisent les 16 premiers bits pour l'adressage réseau. Les bits restant vont désigner les hôtes. Donc dans la classe B, on peut obtenir jusqu'à 2^{16} adresses dans un même réseau.
  Pour reconnaître une adresse IP de la classe B, on vérifie si les deux 1^{ers} bits du 1^{er} octet de l'adresse IP sont = 10, ou bien on vérifie si le 1^{er} nombre décimal de l'adresse est compris entre 128 et 191.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

- **La classe C** : Les adresses IP de la classe C utilisent les 24 premiers bits pour l'adressage réseau. Les bits restant vont désigner les hôtes. Donc dans la classe C, on peut obtenir jusqu'à 2^8 adresses dans un même réseau.
  Pour reconnaître une adresse IP de la classe C, on vérifie si les trois 1^{ers} bits du 1^{er} octet de l'adresse IP sont = 110, ou bien on vérifie si le 1^{er} nombre décimal de l'adresse est compris entre 192 et 223.

Remarque : Le protocole IP est souvent appelé Internet ISO. Il est normalisé sous la norme ISO 8473. Il est utilisé en mode non connecté**.** Par contre, dans les modes orientés connexion, on utilise un protocole (couche 3) appelé X25 et normalisé ISO 8208.

2 - ID Réseau :

L'adresse IP se compose d'une partie réseau et d'une partie hôte. Mais elle comporte une adresse qui ne peut être attribuée à aucune station. Cette adresse est reconnue p ar une série de 0 dans toute la partie hôte. Exemple **: L'adresse 122.5.8.2 est une adresse d'un hôte qui se trouve dans le réseau identifié par l'ID réseau 122.0.0.0**

Les adresses de diffusion : Parfois, on souhaite envoyer des données à toutes les unités d'un réseau en même temps, on utilise alors une adresse de diffusion. C'est une adresse réservée qui contient des valeurs 1 pour l'ensemble des cases concernant les hôtes.
Exemple (classe A) : XXXXXXXX.11111111.11111111.11111111
Décimal : YYY.255.255.255

3 - Les sous réseaux et les masques de sous réseaux :

Parfois pour une meilleure organisation et pour plus de performance on peut décider de subdiviser un réseau en plusieurs sous réseaux. Chaque sous réseau aura sa propre adresse qu'on peut déduire par multiplication de l'adresse IP du réseau par un **masque de sous réseau** (multiplication binaire) .
Un masque de sous réseau est une adresse sur 32 Bits divisée sur 4 octets. Il contient des « 1 » dans la partie réseau et dans la partie sous réseau et des zéros dans la partie hôte. Lorsqu'on connaît la classe d'une adresse IP, on connaît le nombre de Bits réservés pour le réseau et donc on connaît combien de Bits seront utilisés pour le sous réseau.

Exemple : soit l'adresse I.P. :

197-15-22-31 ⟷ 11000101. 00001111. 00010110. 0001111 (classe C)

Soit le masque de sous réseaux suivant :

255-255-255-224 ⟷ 11111111. 11111111. 11111111. 11100000

Réseau : 3x8 bits – classe C

Bits du sous R : 2^3 sous R

L'ID Réseau : 197.15.22.0 ~~Hôte~~

Réseau

4 - Attributions des adresses IP :

Il existe 2 méthodes pour attribuer des adresses IP :

§ **Méthode statique** : un administrateur se déplace de station en station pour donner manuellement des adresses IP.

§ **Méthode dynamique** : Les adresses sont attribuées automatiquement par des protocoles spéciaux : Boot P, DHOP, RARP ….

5 - Fonctionnement des routeurs :

Le routeur décide du meilleur chemin à suivre pour atteindre une station. Il dispose d'un certai n nombre d'interfaces qui vont permettre de le connecter à des réseaux différents. Chaque interface est

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

en contact avec un réseau et porte une adresse IP appartenant au réseau en question. Les réseaux connectés à un même routeur ne peuvent avoir les mêmes adresses.

Remarque : La technique de transmission utilisée au niveau de la couche 3 s'appelle une Technique de commutation de paquets (l'unité de découpe au niveau de la couche 1 –physique- est le bit, au niveau de la couche 2 –liaison- c'est la trame, au niveau de la couche 3 –réseau- c'est le paquet et au niveau de la couche 4 –transport- c'est le segment). Les paquets peuvent suivre des chemins différents mais sont regroupés à l'arrivée .

Serveur Proxy : C'est un logiciel qui s'installe sur un serveur et permet de stocker les pages web sur serveur. Il peut interdire l'accès à certaines pages web et gérer les stations se connectant à Internet .

II-4- LA COUCHE TRANSPORT :

Types de services offerts : Il existe deux types de services offerts:

1 - Services sans connexion

§ **Service sans connexion et sans acquittement :** La machine source envoie les données à la machine destinataire sans recevoir un message de confirmation de la réception (acquittement). Si la trame est perdue, il n'y a pas moyen d'y remédier. Ce type de service est utilisé quand le taux d'erreur est faible et dans le trafic en temps réel (la parole).

§ **Service sans connexion et avec acquittement** : A la réception d'une donnée, le destinataire doit envoyer un acquittement prévenant l'émetteur que le message a été reçu. Si après un certain temps l'émetteur ne reçoit pas cet acquittement, il envoie le message encore une fois.

Le problème dans ce genre de transmission, c'est que le récepteur ait reçu le message, qu'il ait envoyé l'acquittement mais que cet acquittement ait été perdu en route. L'émetteur va envoyer dans ce cas le message plusieurs fois.

2 - Services orientés « connexion »

L'émetteur et le récepteur se mettent d'accord pour établir une connexion avant de transmettre les données. Il faut établir la connexion, transmettre les données et libérer la connexion.

Fonctions de la couche transport : La couche transport permet le contrôle de flux et assure la fiabilité de la transmission. Elle essaie de détecter les erreurs et de redemander la transmission en cas d'erreur. Elle doit découper les messages de grande taille en segments pour le compte de la couche réseau. Du côté récepteur, elle doit ordonner les segments qui sont arrivés pour recomposer le message d'arrivée et le faire passer à la couche session .

La couche transport essaie d'assurer une qualité de service concernant l'établissement d'une connexion, le délai de cette connexion, le débit de l'information et le délai de la déconnexion.

Parmi les protocoles les plus utilisés au niveau de la couche 4, on trouve la pile des protocoles TCP/IP. Ce groupe de protocole comprend les protocoles : IP, TCP/IP et UDT. Le protocole IP est un protocole de couche 3 qui utilise un service sans connexion et qui s'occupe de l'adressage. Le protocole TCP (Transmission Control Protocol) est un protocole de couche 4, utilisant un service orienté connexion et qui assure le contrôle des flux ainsi que la fiabilité. Le mariage de ces 2 protocoles permet d'offrir une

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

bonne qualité de service (c'est sur ce mariage qu'Internet est fondé). Le protocole UDT (User Data Gramm Protocol) est également un protocole de la couche 4 mais utilisant un service sans connexion.

TCP	UDP
§ Orienté connexion § Assure la fiabilité § Division des messages sortants en segments. § Assemblage des segments du côté récepteur. § Nouvel envoi de tout message non reçu .	§ Sans confirmation § Absence de fiabilité § Absence de vérification pour la livraison des segments .

II-5- LA COUCHE SESSION :

Elle assure la communication entre les émetteurs et les récepteurs. Ce genre de communication utilise une technique de commutation de paquet. Ceci implique de nombreuses courtes conversations entre les ordinateurs. La couche session identifie le rôle de chaque station à un moment donné. Elle assure l'ouverture et la fermeture de session entre les applications. En fait, elle contrôle le dialogue et définit les règles d'organisation, de synchronisation, le droit de parole et la reprise de communication après une pause ou une interruption. Cela signifie que chaque interlocuteur doit accepter de respecter un ensemble de règles au cours de la conversation (communication à tour de rôle, simultanée, … etc).

Exemple de protocoles utilisés au niveau de la couche 5 :

SQL : Structured Querry Langage

ASP : Protocole de Session Apple Talk

SCP : Protocole de Contrôle de Session

RPC : Remote Procedure Call

II-6- LA COUCHE PRESENTATION :

Deux personnes s'exprimant dans des langues différentes doivent utiliser les services d'un traducteur. La couche présentation sert de traducteur pour les stations communiquant au niveau d'un réseau. Elle offre trois fonctions principales :

§ Formatage des données

§ Chiffrement des données

§ Compression des données

1 – Si par exemple un système utilise le code ASI I, (American standard Code for EBC DIC : code décimal code binaire étendu) pour la représentation des caractères à l'écran, la couche 6 assure la traduction d'un côté à l'autre. Elle définit également la représentation des images (JPEG , TIFF, GIF , BMP etc.). Elle assure la représentation des graphiques et des sons (WAVE, MIDI, MP3…) et des séquences vidéo (quick time) .

2 – Le chiffrement protège l'information pendant sa transmission. Pour cela, on utilise une clé de chiffrement. La clé va chiffrer les données à la source et les déchiffrer à la destination .

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

3 – Elle a pour objectif de réduire la taille du fichier. Pour réussir cette opération, la couche présentation utilise des Algorithmes qui recherchent les séquences de bits répétitifs et les remplac e par des séquences plus courtes.

II-7- LA COUCHE APPLICATION :

La couche application fournit une interface par laquelle les utilisateurs peuvent entrer en communication avec le réseau. Cette interface peut être directe ou indirecte.

- **Directe** quand il s'agit d'application réseau comme Internet explorer, Netscape Navigator, Telnet (pour la commande des machines à distance), courrier électronique (pour nous permettre d'accéder facilement à des pages Web), IRC (Internet Relay Chat : conversation directe sur Internet) .
- Ou **indirecte** avec des applications autonomes comme les logiciels de traitement de texte, les tableurs, les gestionnaires d'impression, l'explorateur … etc. Ce genre d'applications utilise un redirecteur qui est un logiciel qui permet de dirig er les demandes s'adressant à l'extérieur de la machine vers le réseau .

Remarque : Le serveur de nom de domaine (Domaine Name Server) est un dispositif réseau qui gère les noms des domaines et converti ces noms on adresse IP. Un nom de domaine est une ch aîne de caractères ou de chiffres généralement une abréviation représentant un site Internet : les systèmes DNS (Domaine Name Server) sont dotés d'une structure hiérarchique et de tables de recherche très sophistiquées .

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

CONTROLE CONTINU N° 1

Question 1 : Question: Les unités d'interconnexion de réseaux sont utilisées pour relier des _____.

A.réseaux locaux à d'autres réseaux locaux
B.réseaux locaux à des réseaux longue distance
C.réseaux longue distance à d'autres réseaux longue distance
D.toutes ces réponses

Question 2 : Question: Quelle partie d'un réseau fournit des applications et des données aux ordinateurs hôtes?

A.Serveur
B.Concentrateur
C.Routeur
D.Pont

Question 3 : Question: Les clients et les serveurs fonction nent au niveau de combien de couches OSI?

A.Quatre
B.Cinq
C.Six
D.Sept

Question 4 : Question: A quoi sert une carte réseau?

A.Etablit, gère et ferme les sessions entre des applications, et gère l'échange de données entre les entités de la couche de présentation.
B.Donne à l'hôte accès au média.
C.Fournit des services aux processus d'application.
D.Fournit des mécanismes d'établissement, de maintien et de coupure de circuits virtuels, de reprise et de contrôle du flux d'information.

Question 5 : Question: Quelle couche du modèle OSI décrit le média de réseautage?

A.Couche réseau
B.Couche liaison de données
C.Couche physique
D.Couche de transport

Question 6 : Question: Quel matériau est utilisé pour le média de réseau?

A.fil
B.câble
C.fibre optique
D.toutes ces réponses

Question 8 : Question: Répéteur multiport est un autre nom pour désigner un _____.

A.Pont
B.Hôte
C.Concentrateur
D.Séquenceur

Question 9 : Question: Lequel des énoncés suivants e st vrai concernant les ponts et leurs décisions d'acheminement?

A.Ils fonctionnent à la couche 2 et utilisent les adresses IP pour prendre des décisions.
B.Ils fonctionnent à la couche 3 et utilisent les adresses IP pour prendre des décisions.
C.Ils fonctionnent à la couche 2 et utilisent les adresses MAC pour prendre des décisions.
D.Ils fonctionnent à la couche 3 et utilisent les adresses MAC pour prendre des décisions.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Question 10 : Question: Lequel des énoncés suivants est vrai concernant l es commutateurs et leurs décisions d'acheminement?

A.Ils fonctionnent à la couche 2 et utilisent les adresses IP pour prendre des décisions.
B.Ils fonctionnent à la couche 3 et utilisent les adresses IP pour prendre des décisions.
C.Ils fonctionnent à la couche 2 et utilisent les adresses MAC pour prendre des décisions.
D.Ils fonctionnent à la couche 3 et utilisent les adresses MAC pour prendre des décisions.

Question 11 : Question: Lequel des énoncés suivants est vrai concernant le rôle d'un c ommutateur?

A.Concentre la connectivité.
B.Combine la connectivité d'un concentrateur à la régulation du trafic d'un pont.
C.Commute les données des ports d'entrée aux ports de sortie.
D.Toutes ces réponses

Question 12 : Question: Que connectent les routeurs?

A.Les ponts et les répéteurs
B.Les ponts et les concentrateurs
C.Deux réseaux ou plus
D.Les concentrateurs et les nœuds

Question 13 : Question: Sur les grands réseaux, quels sont les plus importants dispositifs de régu lation du trafic?

A.Concentrateurs
B.Serveurs
C.Routeurs
D.Ponts

Question 14 : Question: Bien que les réseaux d'ordinateurs existent depuis longtemps, quelle décennie a été le témoin des progrès importants que représentent les passerelles et les routeurs?

A.1960
B.1970
C.1980
D.1990

Question 15 : Question: Le Web a vu le jour au cours de quelle décennie?

A.1960
B.1970
C.1980
D.1990

Question 16 : Question: Les routeurs fonctionnent principalement à quelle couche du mod èle OSI?

A.Couche 1
B.Couche 2
C.Couche 3
D.Couche 4

Question 17 : Question: Quel est l'ordre d'encapsulage?

A.Données, segment, paquet, trame, bits
B.Données, trame, paquet, segment, bits
C.Bits, données, paquet, trame
D.Bits, tra me, données, paquet

Question 18 : Question: Les unités de couche 1 examinent les :

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

A.Bits
B.Trames
C.Paquets
D.Toutes ces réponses

Question 19 : Question: Laquelle des unités suivantes n'est PAS une unité de couche 1?

A.Concentrateur
B. Répéteur
C.Commutateur
D.Emetteur-récepteur

Question 20 : Question: Les ponts prennent des décisions en examinant quoi?

A.Adresses de couche 2
B.Adresses de couche 3
C.Information de couche 4
D.Information de couche 7

Question 21 : Question: On considère les routeurs comme des unités de couche _____.

A.Un
B.Deux
C.Trois
D.Quatre

Question 22 : Question: Quelle unité parmi les suivantes pourrait être considérée comme une unité de couche 1 à 7?

A.Routeur
B.Concentrateur
C.Commutateur
D.Ordinateur

Question 23 : Question: Pour créer un réseau à partir de deux PC seulement, quel genre de câble utilise -t-on pour les raccorder?

A.RG7U
B.Câble coaxial
C.Câble à fibre optique
D.Câble d'interconnexion

Question 24 : Question: Pour créer un réseau local simple de quatre ordinateurs, vous utiliseriez un(e) _____ pour les raccorder.

A.câble d'interconnexion
B.ligne série
C.concentrateur
D.routeur

Question 25 : Question: Si quatre hôtes sont connecté s à un concentrateur, puis à Internet, combien faut -il d'adresses IP pour ces cinq unités?

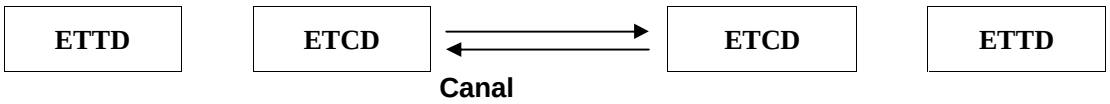
A.Un
B.Deux
C.Quatre
D.Cinq

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

III- PROTOCOLE DE COMMUNICATION

III-1- DEFINITION

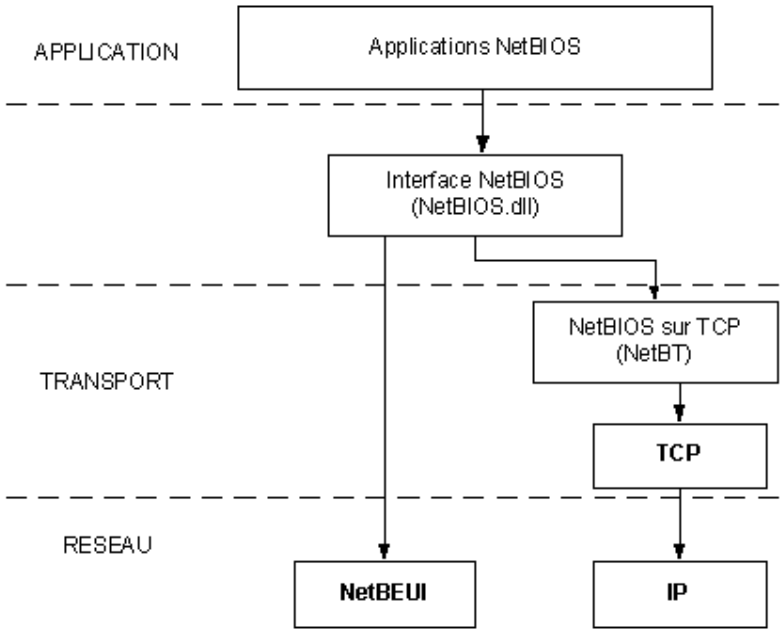
la transmission suppose une source de données et un récepteur de données commu niquant à travers un canal de transmission. Source et récepteur sont des terminaux officiellement appelés **ETTD** (exemple : ordinateur)
La connexion des terminaux (ETTD) au canal nécessite généralement une adaptation qui sera réalisée par un ETCD. Les ETCD permettent d'adapter le flux de données aux conditions de la ligne et de faire les transformations Analogique ⟶ Numérique ou Numérique ⟶ Analogique



Pour qu'une transmission se déroule co nvenablement entre deux éléments, il faut que les composantes de la chaîne (ETTDs, ETCDs, canal) suivent les procédures et les conventions qui constitueront la grammaire du dialogue. Ce sont ces conventions que l'on appelle protocole.

III-2- LE PROTOCOLE NETBIOS ET NETBEUI

Windows 9x et NT utilise le protocole propriétaire Netbeui pour communiquer avec d'autre machine Windows. Ce protocole a été abandonné dans Windows 2000, ce qui explique en partie les difficultés à mettre sur un même réseau des machines NT et 2000
D'ailleurs, pour les réseaux de petite taille, une vingtaine de postes, cette solution permet un partage simple des ressources. Cette solution permet aux **applications NETBIOS** d'accéder au réseau en.



s'appuyant sur le **protocole NETBEUI**.

NetBIOS : (Network Basic Input/output System) Interface de programmation qui permet aux applications d'accéder au réseau local.
NetBIOS utilise un service de noms pour contrôler les échanges de point à point.

NetBEUI : (NetBIOS Extended User Interface) est le protocole de transport des réseaux Windows. Il ne peut pas être routé et repose principalement sur les diffusions.

NetBT (NetBIOS sur TCP/IP) est le service de réso lution de noms NetBIOS pour les réseaux Windows sous TCP/IP
Le protocole Netbios peut être utilisé indifféremment sur la couche MAC et sur la couche TCP/IP lorsque celle-ci existe. Sur le réseau local (même sous-réseau IP), un simple broadcast (sur UDP) permet chaque minute, à chaque machine du réseau, de signaler qu'elle est toujours présente sur le réseau. Si la machine n'est pas équipée de la pile TCP/IP,

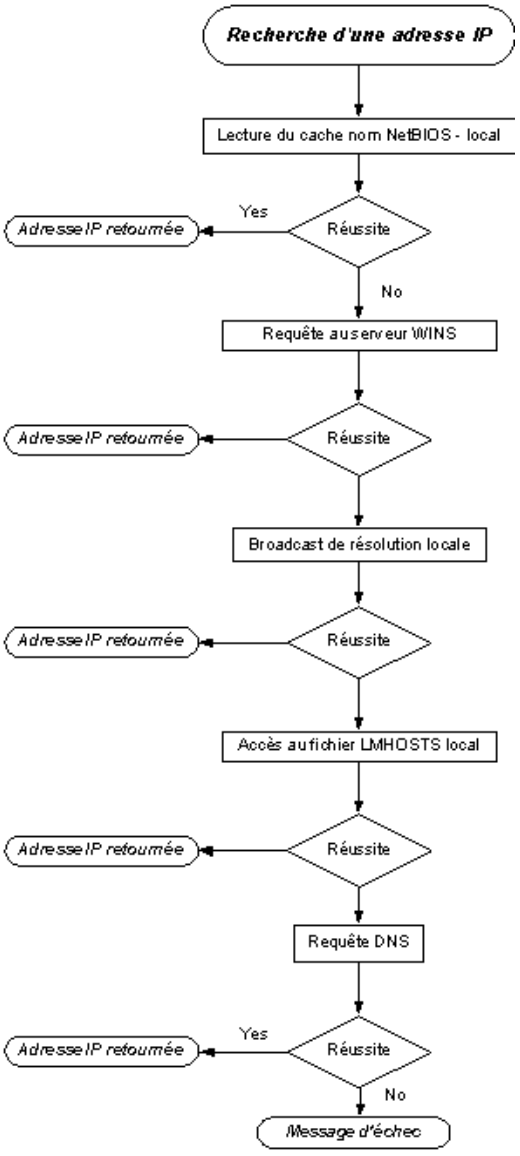
Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

les échanges entre les machines d'un même sous-réseau s'effectuent directement sur la couche MAC, et pour les discussions entre réseau différent, il est possible de l'utiliser sur la couche TCP/IP

Recherche d'adresse IP sous Windows NT :

La connexion entre ordinateurs Windows est précédée d'une mise en correspondance d'un nom NetBIOS et de l'adresse IP. Windows NT propose différentes méthodes de résolution de noms permettant aux ordinateurs d'établir une connexion :
- la diffusion IP.
- le mappage statique, à l'aide d'un fichier LMHOSTS local.
- le serveur de noms NetBIOS : WINS.
- le serveur de noms DNS.

Plus simplement, lorsque vous faîtes la commande "ping toto", la machine cherche à connaître l'adresse IP de toto pour savoir à qui envoyé sa trame. Pour une plus grande efficacité les postes clients WINS conjuguent par défaut ces différentes méthodes de résolution en suivant le schéma ci-dessous :



Chaque machine Windows a un nom Netbios. C'est le "nom de la machine" que l'on retrouve dans le premier onglet des paramètres réseaux.

Lorsque vous tentez de joindre une machine sur le réseau (si vous faites un "ping toto", par exemple), le système commence par **rechercher ce nom dans son cache** pour voir si une conversation a déjà eu lieu avec cette machine peu de temps avant. Si c'est le cas, l'adresse IP a été gardée dans le cache (et est donc connue) et l'échange peu avoir lieu.

Le cas échéant, la machine tendre de **faire appel au serveur WINS**. WINS (WIndows Name Server), fonctionne comme un serveur DNS, mais il s'agit encore une fois d'un système propriétaire Microsoft. Le serveur WINS est une machine qui associe les noms Netbios et les adresses IP du réseau, et lorsque ce système est utilisé, vous pouvez renseigner l'adresse IP du serveur WINS dans les paramètres TCP/IP de votre machine. Dans ce cas, votre machine peut questionner ce serveur afin de savoir si la machine recherchée est connue. Si le serveur WINS connait la machine, il retourne l'adresse IP, sinon, le système fait un broadcast en résolution locale.

Le broadcast en résolution locale est une opération très simple qui consiste à envoyer une trame à tous les hôtes du réseau local pour demander si la machine recherchée est présente sur le réseau. Si la machine est sur le réseau, elle peut répondre directement à l'intéressé, sinon, on utilise le fichier LMHOST.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Le fichier LMHOST (C:\WIN NT\System32\Drivers\etc\lmhost) permet d'associer des noms à des adresses IP manuellement de façon à définir vos propres noms. Ce fichier est chargé à l'allumage de votre PC, aussi n'oubliez pas de redémarrer votre machine pour que les modifications du fichier soient prises en compte. N'oubliez pas non plus d'activer le service de scrutation LMHOST dans les paramètres TCP/IP.

Si la machine n'est pas renseignée dans le fichier LMHOST, la dernière opération consiste à faire une requête auprès du **serveur DNS.**

III-3- LE PROTOCOLE TCP :

Le protocole TCP est défini dans le but de fournir un service de transfert de données de haute fiabilité entre deux ordinateurs "maîtres" raccordés sur un réseau de type "paquets commutés", et sur tout système résultant de l'interconnexion de ce type de réseaux.

Caractéristiques

TCP est un protocole orienté connexion conçu pour s'implanter dans un ensemble de protocoles multicouches, supportant le fonctionnement de réseaux hétérogènes. TCP fournit un moyen d'établir une communication fiable entre deux tâches exécutées sur deux ordinateurs autonomes raccordés à un réseau de données.
Le protocole TCP s'affranchit le plus possible de la fiabilité intrinsèques des couches inférieures de communication sur lesquelles il s'appuie. TCP suppose donc uniquement que les couches de communication qui lui sont inférieures lui procurent un service de transmission de paquet simple, dont la qualité n'est pas garantie.
TCP s'intègre dans une architecture multicouche des protocoles, juste au -dessus du protocole Internet IP. Ce dernier permet à TCP l'envoi et la réception de segments de longueur variable, encapsulés dans un paquet Internet appelé aussi "datagramme". Le datagramme Internet dispose de mécanismes permettant l'adressage des services TCP source et destination, quelle que soit leur position dans le réseau. Le protocole IP s'occupe aussi de la fragmentation et du réassemblage des paquets TCP lors de la traversée de réseaux de plus faibles caractéristiques.

Le datagramme IP transporte aussi les informations de priorité, fragmentation relatives aux segments TCP.

Interfaces

TCP fournit un service de communication de processus à processus, dans un environnement réseau, il est défini comme un protocole de communication "host to host", c'est à dire de maître à maître (par opposition à "central à terminal"). TCP s'interface avec un processus utilisateur ou applicatif et un protocole de niveau inférieur du type Internet Protocol.

L'interface avec les applicatifs consiste en un ensemble de commandes comme le ferait une application à un système d'exploitation pour la manipulation de fichiers. Par exemple, on trouvera des commandes pour établir et rompre une communication, pour envoyer ou recevoir des données sur une connexion ouverte.
TCP assume un fonctionnement avec un large ensemble de protocoles réseau. Dans ce document, nous nous limiterons au fonctionnement avec IP.

Fonctionnement

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

TCP est conçu pour fournir un service de transmission de données fiable entre deux machines raccordées sur un réseau de paquets. Pour pouvoir assurer ce service même au dessus d'une couche de protocole moins fiable, les fonctionnalités suivantes sont nécessaires:
- Transfert de données de base
- Correction d'erreur
- Contrôle de flux
- Multiplexage
- Gestion de connexions
- Priorité et Sécurité

Ces fonctionnalités sont décrites en dans les paragraphes qui suivent.

Transfert de données de base

TCP est capable de transférer un flux continu de données entre deux ordinateurs, en découpant ce flux en paquets . En général, TCP décide de lui -même là où le flux de données doit être coupé.
Parfois les utilisateurs ont besoin de savoir que toutes les données soumises à TCP ont bien été émises. La fonction "push" a été prévue a cet effet. Pour s'assurer de la transmission complète de données jusqu'à un point spécifié, l'utilisateur activera la fonction "push" de TCP. Cette fonction oblige TCP à transmettre rapidement les données situées avant le point spécifié vers le destinataire. Il n'est nul besoin de fournir un marqueur spécifique pour ce point, dans la mesure ou le destinataire accepte ces données comme une transmission normale.

Contrôle d'erreur

TCP doit considérer et traiter les cas de données perdues, erronées, dupliquées, ou arrivées dans le désordre à l'autre bout de la liaison Internet. Ceci est réalisé par l'insertion d'un numéro de séquence, et par l'obligation d'émission d'un "accusé de réception" (ACK) par le TCP destinataire. Si l'accusé de réception n'est pas reçu au bout d'un temps prédéfini, le paquet sera réémis. Côté récepteur, les numéros de séquence sont utilisés pour reconstituer dans le bon ordre le flux original, et éliminer les paquets dupliqués. L'élimination des erreurs physiques de transmission se fait par encodage d'un Checksum à l'émission, recalcul de ce Checksum par le destinataire, et élimination des paquets pour les quels les deux valeurs ne correspondent pas.
Tant que TCP fonctionne correctement, et que le réseau Internet n'est pas saturé, aucune faute de transmission ne devrait transparaître dans la communication. TCP est donc sensé récupérer les erreurs de la transmission Internet.

Contrôle de flux

TCP fournit un moyen au destinataire pour contrôler le débit de données envoyé par l'émetteur. Ceci est obtenu en retournant une information de "fenêtre" avec chaque accusé de réception indiquant la capacité de réception instantanée en termes de numéros de séquence. Ce paramètre noté "window" indique le nombre d'octets que l'émetteur peut envoyer avant une autorisation d'émettre ultérieure.

Multiplexage

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Pour permettre à plusieurs tâches d'une même machine de communiquer simultanément via TCP, le protocole définit un ensemble d'adresses et de ports pour la machine. Une "socket" est défini par l'association des adresses Internet source, destinataire, ainsi que les deux numéros de port à chaque extrémité. Une connexion nécessite la mise en place de deux sockets. Une socket peut être utilisée par plusieurs connexions distinctes.
L'affectation des ports aux processus est établie par chaque ordinateur. Cependant, il semble judicieux de réserver certains numéros de ports pour des services caractérisés et souvent utilisés. Ces services standards pourront alors être atteints via ces ports "réservés". L'affectation, l'utilisation et l'apprentissage des ports associés à d'autres services moins courants ou propriétaires nécessitera l'utilisation de mécanismes plus dynamiques.

Connexions

Les mécanismes de fiabilisation et de contrôle de flux décrits ci-dessus imposent à TCP l'initialisation et la maintenance de certaines informations pour chaque communication. La combinaison de ces informations, dont les sockets, les fenêtres, et les numéros de séquence formeront ce que nous appelons une connexion. Chaque connexion est identifiée de manière unique par sa paire de sockets, définissant chacun des deux sens de la communication. Lorsque deux processus désirent communiquer, leur TCP respectifs doivent tout d'abord négocier et établir une connexion (initialiser ces informations d'état de part et d'autre). Lorsque la communication s'achève, elle sera fermée, en libérant ses ressources à d'autres usages.
Dans la mesure où l'on considère que les ordinateurs, ainsi que le réseau Internet n'est pas d'une fiabilité absolue, on utilise une méthode d'initialisation par négociation bilatérale basée sur une horloge pour les numéros de séquence.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

IV- LE PROTOCOLE TCP/IP

IV-1- ADRESSE IP :

Au niveau de la couche **Liaison**, les nœuds du réseau communiquent avec les autres stations en utilisant des adresses qui dépendent du type de réseau utilisé. Un nœud peut être un micro -ordinateur, un serveur de fichier, une imprimante réseau ou n'importe quel périphérique utilisant TCP/IP. Chaque nœud possède une adresse **physique** ou adresse **MAC** .
Dans les réseaux Ethernet et Token-Ring, l'adresse physique est contenue dans une ROM sur chaque interface réseau. Toutes les adresses sont différentes et comportent 6 octets. Cette adresse est déterminée par le constructeur de l'interface selon un plan de numérotation à l'échelle mondiale.
Dans le réseau X25, l'adresse déterminée par le concessionnaire du réseau comporte au maximum 15 chiffres décimaux.
Dans le réseau LocalTalk d'Apple, l'adresse comporte un octet pour déterminer le numéro du réseau et 2 pour déterminer le numéro de la station.

Généralités :

Les adresses **IP** au contraire sont des adresses logiques. Elles sont **indépendantes du type de réseau** utilisé. Dans la version 4 de IP, elles comportent toujours **32 bits**, dont une partie identifie le réseau (**NetID**), l'autre le nœud sur ce réseau (**HostID**).

Types d'adresses :

- **Unicast** : Adresse permettant l'adressage d'une **seule** machine.
- **Multicast** : Adresse correspondant à un **groupe** de machines.
- **Broadcast** : Adresse correspondant à **toutes** les machines d'un réseau.

Représentation des adresses IP :

La représentation de cette adresse se fait dans une notation " **décimale pointée**" (dotted-decimal notation), c'est-à-dire que chaque octet de l'adresse est représenté par un nombre décimal, séparé du suivant par un point. Par exemple :

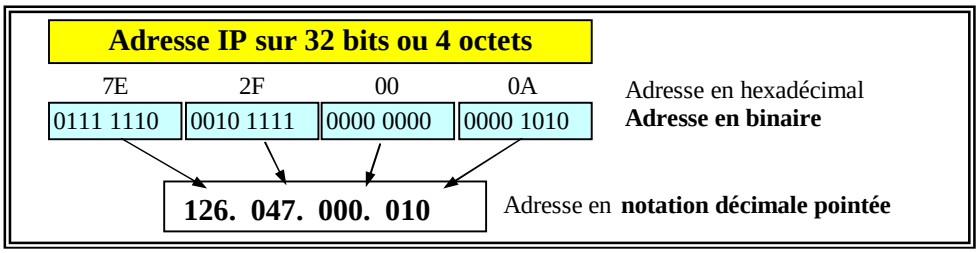


Figure : Adresses IP. Notation décimale pointée.

Parfois, la représentation se fait en Hexadécimal de la façon suivante : **? x7E.? x2F.? x00.? x0A**

Classes d'adresses :

Il existe 5 classes d'adresses IP.

1) Classe A

Dans cette classe, l'adresse réseau est définie sur **7 bits** et l'adresse hôte sur **24 bits**.

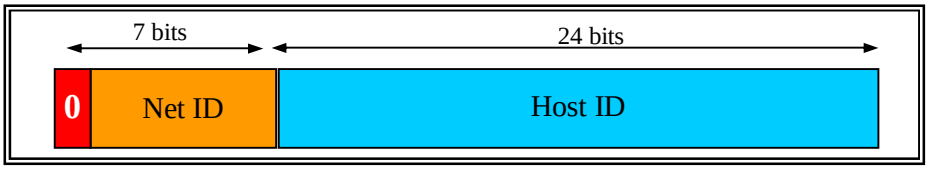


Figure : Adressage IP Classe A.

2) Classe B

Dans cette classe, l'adresse réseau est sur 14 bits et l'adresse hôte sur 16 bits .

MAC = Medium Access Control

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

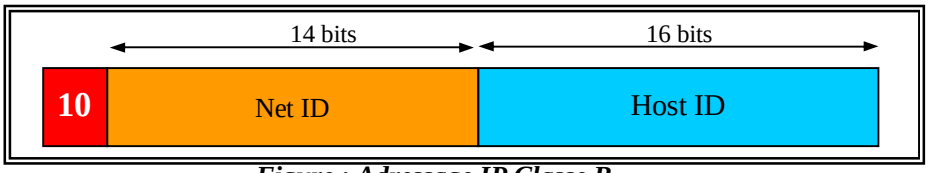


Figure : Adressage IP Classe B.

3) Classe C

Dans cette classe l'adresse du réseau est codifiée sur 21 bits et l'adresse hôte sur 8 bits

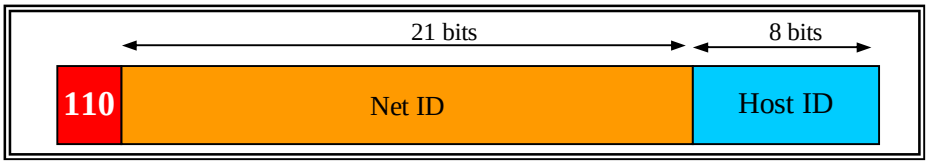


Figure : Adressage IP Classe C.

Pour faciliter le routage les adresses IP de classe C correspondent à de s emplacements géographiques :

Adresses	Zone géographique
192.0.0 à 193.255.255	Adresses allouées avant la répartition géographique. Elles correspondent donc à plusieurs régions.
194.0.0 à 195.255.255	Europe
198.0.0. à 199.255.255	USA
200.0.0 à 201.255.255	Amériques centrale et du Sud
202.0.0 à 203.255.255	Pacifique

4) Classe D

Dans cette classe l'adresse du réseau est codifiée sur 28 bits et sert à diffuser des trames vers des groupes de stations.

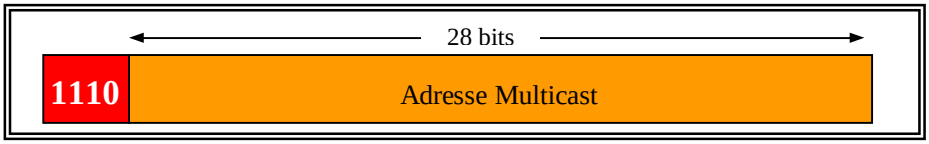


Figure : Adressage IP classe D

5) Classe E

Cette classe est réservée à un usage futur.

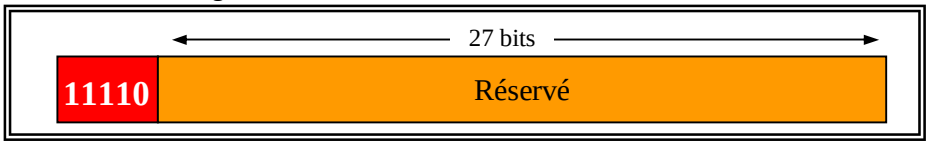


Figure : Adressage IP Classe E.

6) Identification des classes d'adresses

Selon la valeur des bits du premier octet représentant l'adresse réseau IP, il est facile de déterminer la classe utilisée.

Classe	Gamme en notation décimale	Premier octet en binaire	Nb de réseaux	NB de noeuds
A	0.0.0.0 à **127**.255.255.255	**0** 0000000 et **0** 1111111	**126**	**16 777 214**
B	**128**.0.0.0 à **191**.255.255.255	**10** 000000 et **10** 111111	**16383**	**65534**

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

C	**192**.0.0.0 à **223**.255.255.255	**110** 00000 et **110** 11111	**2 097 151**	**254**
D	**224**.0.0.0 à **239**.255.255.255	**1110** 0000 et **1110** 1111		
E	**240**.0.0.0 à **247**.255.255.255	**11110** 000 et **11110** 111		

Figure : Gammes d'adresses IP en fonction des classes.

7) Adresses Privées

Pour les réseaux non connectés à l'Inter net, les administrateurs décident de la classe et de l'adresse NetID. Cependant pour des évolutions possibles, il est fortement recommandé de servir des adresses non utilisées sur Internet. Ce sont les adresses **privées** suivantes en classe A, B et C :

Tranches d'adresses IP privées	Nombre de réseaux privés
10.0.0.0 à 10.255.255.255	1 réseau de classe A
172.16.0.0 à 172.31.255.255	16 réseaux de classe B
192.168.0.0 à 192.168.255.255.	256 réseaux de classe C

Figure : Adresses privées

8) Adresses spéciales

Les règles concernant les adresses IP prévoient un certain nombre d'adresses spéciales :

- Adresses **Réseaux** : Dans ces adresses, la partie réservée à l'adresse station est à 0. Par exemple, 126.0.0.0 représente l'adresse réseau et non l'adresse d'un hôt e.
- Adresses **Broadcast** à diffusion dirigée : Dans ces adresses, la partie "adresse Station" a tous ses bits à **1**. Par exemple, 126.255.255.255 est une adresse de broadcast sur le réseau 126. Les routeurs peuvent transmettre cette trame vers le réseau 126.
- Adresses **Broadcast** à diffusion limitée. Dans ces adresses tous les bits sont à 1. (255.255.255.255) à. Cette trame est limitée au réseau de l'hôte qui l'envoie.
- Adresses pour la **maintenance** ou adresses "Loopback" : 127.0.0.1 (Ping sur la station pour v érifier le fonctionnement de la pile IP locale).
- Adresses **réservées** : Ce sont les adresses dont le numéro de réseau n'est composé que de 0 ou de 1.

IV-2- RESEAUX ET SOUS-RESEAUX

Un réseau peut être divisé en sous-réseaux afin de pouvoir :

- éviter le gaspillage des adresses nœuds d'un réseau
- utiliser des supports physiques différents.
- réduire le trafic sur le réseau.
- isoler une partie du réseau en cas de défaillance d'un composant du réseau.
- augmenter la sécurité.

Chaque sous-réseau est relié à un autre par un routeur.

Exemple :

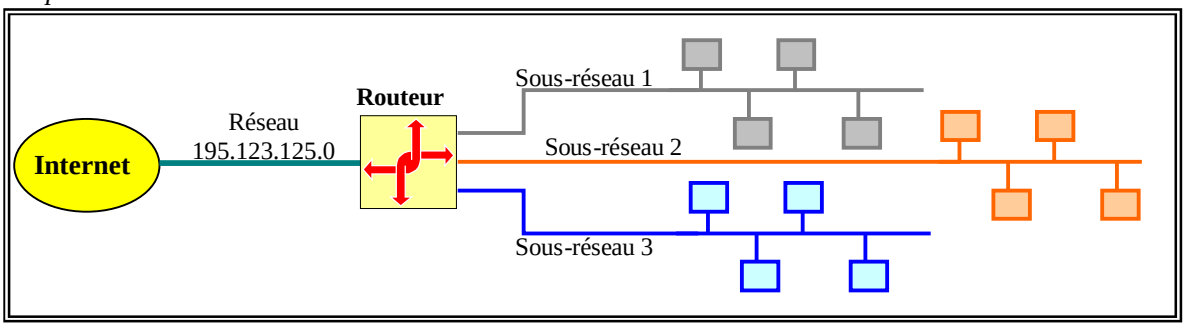


Figure : Sous-réseaux.

Dans la figure ci-dessus, le routeur est connecté à Internet par un réseau de classe **C** 195.123.125.0. Il est donc possible d'utiliser 256 (- 2) adresses pour les nœuds. Cependant si t ous les nœuds sont sur le même réseau, celui-ci risque d'être chargé. On répartit les nœuds sur 3 réseaux que l'on connecte à un routeur. Chacun de ces réseaux devant avoir une adresse distincte, on crée des adresses de sous - réseaux pour chacun d'eux.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Masques de sous-réseaux

La notion de sous-réseaux était inexistante au début de IP. Elle est apparue avec la RFC 950 vers 1985. L'adressage de sous-réseaux va se faire avec des bits normalement réservés à l'adressage des nœuds.

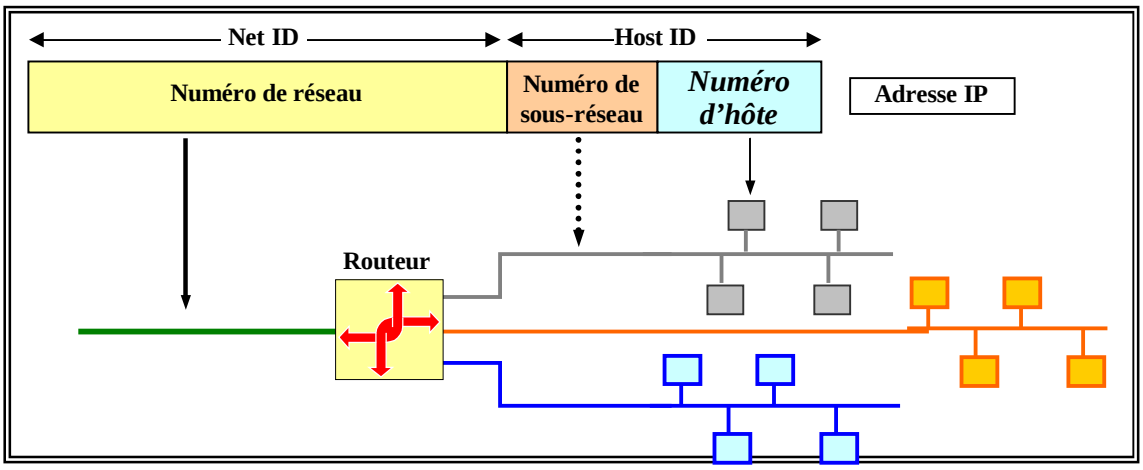


Figure : Numérotation des sous-réseaux.

Pour indiquer le nombre de bits pris sur la partie HostID comme numéro de sous -réseau, on va utiliser un masque de sous-réseaux. Ce masque indique par des **bits à 1** le nombre de bits de l'adresse IP qui correspondent à l'adresse réseau et à l'adresse sous-réseaux. Les **bits à 0** du masque indiquent les bits de l'adresse IP qui correspondent à l'HostID

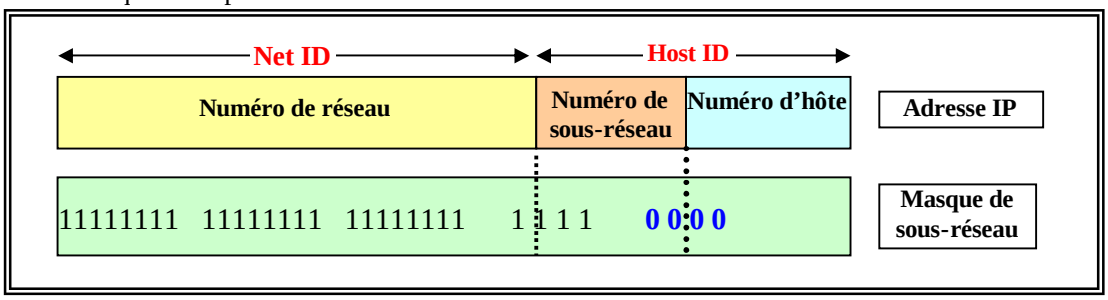


Figure : Masque de sous-réseau.

Dans l'exemple ci-dessus, l'adresse IP est une adresse de classe C. On désire créer 16 sous-réseaux. Il est donc nécessaire d'utiliser 4 bits de la partie HostID pour indiquer le numéro de sous -réseau.
Le masque comporte **28** bits à **1**, c'est à dire :

- **24** bits correspondant à la partie NetID de l'adresse et **4** bits pour indiquer les bits de l'adresse IP qui doivent être interprétés comme étant l'adresse de sous -réseaux.
- **4** bits à **0**, indiquent les bits de l'adresse IP qui doivent être interprétés comme des adresses de nœuds.

Les masques de sous réseaux sont à entrer dans chaque o rdinateur travaillant en IP. Les valeurs des masques se rentrent la plupart du temps en notation décimale pointée. Pour illustrer l'exemple ci -dessus, voici comment il conviendrait d'indiquer à une station NT, son adresse IP et son masque de sous-réseau.

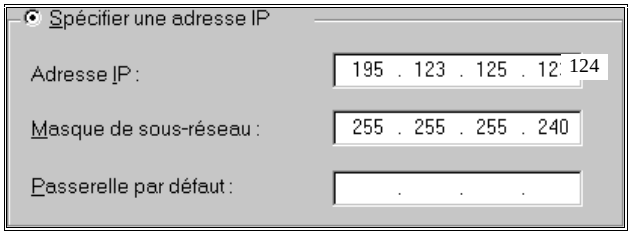
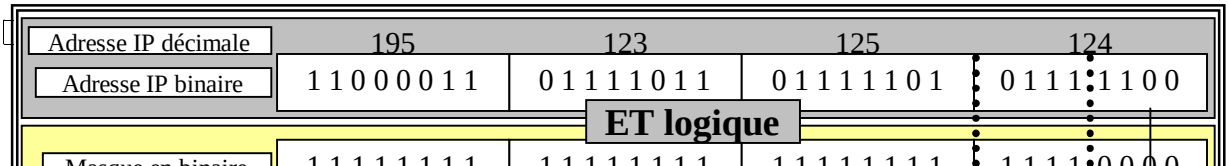


Figure : Entrées de l'adresse IP et du masque de sous -réseau.



Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Figure : Calcul de l'adresse de sous-réseau et de l'adresse nœud.

Dans cet exemple, le masque de sous-réseau comporte **28 bits**. L'adresse IP 195.123.125.124 est une adresse de classe C.

Les **24 premiers bits** du masque correspondent au **NetID**.

Les **4 bits** suivants à **1** dans le masque indiquent qu'il faut interpréter les 4 premiers bits du dernier octet comme une **adresse de sous-réseau** et non comme une adresse HostID. Les 4 bits à 0 du masque indiquent qu'il faut interpréter les 4 derniers bits du dernier octet de l'adresse IP comme une adresse nœud.

On calcule l'adresse du sous-réseau en tenant compte du poids binaire de chaque bit. Ici, (128 x 0) + (1 x 64) + (1 x 32) + (1 x 16)= 112. L'adresse nœud correspond aux 4 derniers bits de l'adresse IP (12).

Exemple en classe B:

	Masque-->	**11111111 . 11111111 . 1111**	***0000 . 00000000***	ID ss-réseau	ID nœud
Adresses IP	129.047.192.254	10000001 . 00101111 . 1100	*0000 . 11111110*		
	129.047.193.001	10000001 . 00101111 . 1100	*0001 . 00000001*		
	129.047.192.001	10000001 . 00101111 . 1100	*0000 . 00000001*		
	129.047.128.001	10000001 . 00101111 . 1000	*0000 . 00000001*		
	129.047.129.001	10000001 . 00101111 . 1000	*0001 . 00000001*		
	129.047.128.254	10000001 . 00101111 . 1000	*0000 . 11111110*		

Figure : Exemple de masque de sous-réseaux avec des adresses de classe B.

Quelle est la valeur du masque en décimal. ? ……..
Quel est pour toutes les adresses IP le numéro de réseau ? ……..
Complétez le tableau en rentrant les adresses de sous-réseaux et les adresses nœud pour chaque adresse IP .

Exemple en classe C :
Un masque de sous-réseau est **255.255.255.240**
Quelle est la classe des adresses IP qui sont utilisées dans le tableau ci-dessous ? .....
En face des adresses IP suivantes, indiquez l'ID sous-réseau puis l'ID nœud :

Adresse IP	**ID sous-réseau**	**ID nœud**
195.252.13.33		
195.252.13.66		
195.252.13.47		

Figure : Exemple de masque de sous-réseau en classe C.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

IV-3- LES SERVICES D'APPLICATION UTILISANT TCP :

Des applications réseau sont directement liées à la pile de protocole TCP/IP et la version "client" de ces applications est souvent livrée avec la pile de protocoles. Ces a pplications permettent par exemple le transfert de fichier (FTP), l'émulation de terminal en réseau (Telnet), l'affichage de page HTML (serveur et navigateur WEB), fonctions de nommage (DNS), …
Suivant les cas et le besoin de fiabilité des applications, el les utilisent soit le protocole **TCP,** soit le protocole **UDP** comme protocole de transport.

Ping :

Ping (Packet Internet Grouper) est une application qui permet de vérifier le bon fonctionnement des composants d'un réseau utilisant TCP/IP. Elle permet par es sais successifs de tester la pile IP et l'interface réseau de l'ordinateur sur lequel on se trouve, puis de tester les liaisons avec les autres machines du réseau. Cette application utilise le protocole ICMP véhiculé par IP.

Commande Ping avec paramètres demandant 5 envois de trames d'une longueur de 1000 octets. vers la machi ne dont @IP est 126.0.0.1

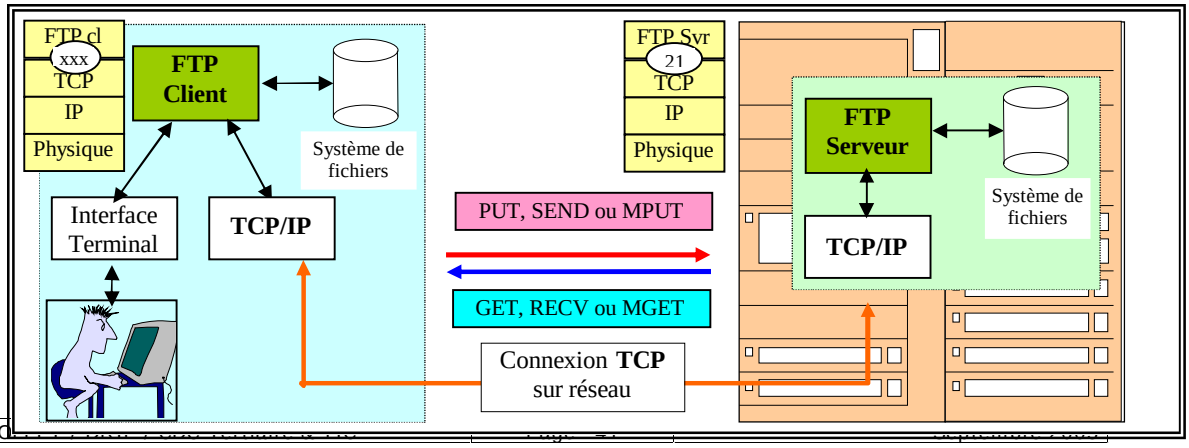
```
# ping -c5 -s1000 126.0.0.1
PING 126.0.0.1 (126.0.0.1): 1000 data bytes
1008 bytes from 126.0.0.1: icmp_seq=0 ttl=255 time=14 ms
1008 bytes from 126.0.0.1: icmp_seq=1 ttl=255 time=14 ms
1008 bytes from 126.0.0.1: icmp_seq=2 ttl=255 time=14 ms
1008 bytes from 126.0.0.1: icmp_seq=3 ttl=255 time=14 ms
1008 bytes from 126.0.0.1: icmp_seq=4 ttl=255 time=14 ms
----126.0.0.1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 14/14/14 ms
```

Statistiques de fin . Les trames ont mis en moyenne 14 ms pour faire l'aller et retour entre les 2 machines. Tous les paquets ont été retransmis.

Figure : Commande Ping.

FTP :

FTP (port 21) est une application qui permet d'assurer le transfert de fichiers, sans erreur, entre un micro-ordinateur et un hôte ou entre 2 hôtes. Un certain nombre de commandes propres à cette application permettent des transferts uniques ou multiples de fichiers dans les 2 sens (à l'alternat).



Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Figure : FTP.

Il existe une application FTP en mode client côté utilisateur. Dans l'autre ordinateur, une application FTP serveur tourne en tâche de fond.

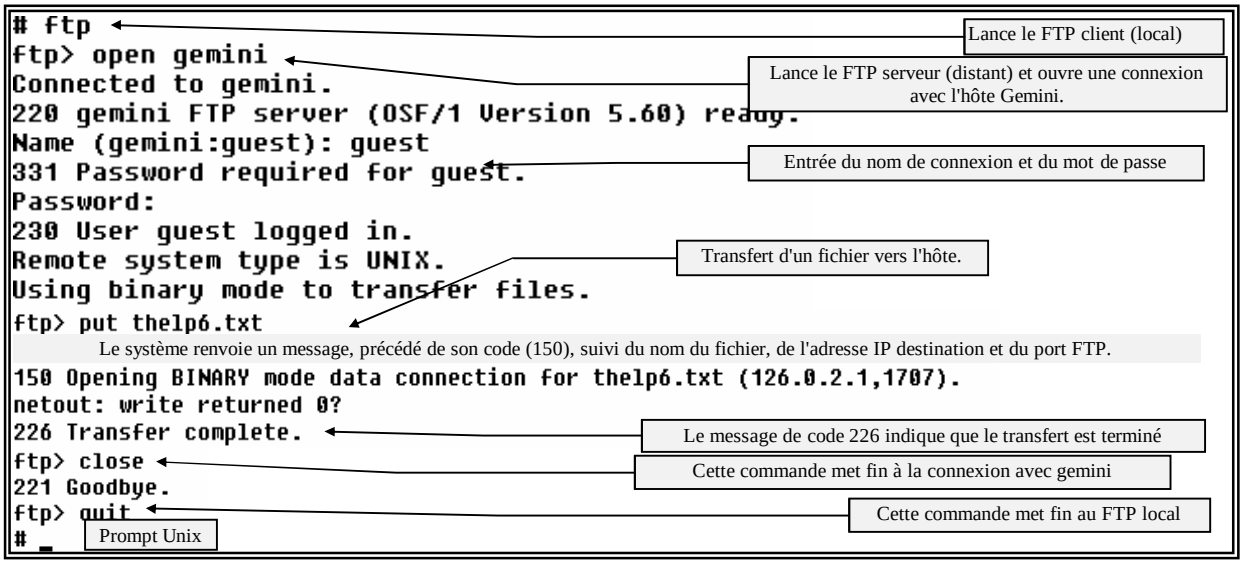

ftp
Lance le FTP client (local)
ftp> open gemini
Connected to gemini.
220 gemini FTP server (OSF/1 Version 5.60) ready.
Lance le FTP serveur (distant) et ouvre une connexion avec l'hôte Gemini.
Name (gemini:guest): guest
331 Password required for guest.
Password:
Entrée du nom de connexion et du mot de passe
230 User guest logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
Transfert d'un fichier vers l'hôte.
ftp> put thelp6.txt
Le système renvoie un message, précédé de son code (150), suivi du nom du fichier, de l'adresse IP destination et du port FTP.
150 Opening BINARY mode data connection for thelp6.txt (126.0.2.1,1707).
netout: write returned 0?
226 Transfer complete.
Le message de code 226 indique que le transfert est terminé
ftp> close
Cette commande met fin à la connexion avec gemini
221 Goodbye.
ftp> quit
Cette commande met fin au FTP local
_
Prompt Unix

Figure : Commandes FTP.

Telnet

Telnet (port 23) est un protocole qui permet **d'émuler** à partir d'un **micro-ordinateur** un **Terminal** connecté sur un Hôte à travers le **réseau**. Le type de terminal émulé peut être choisi dans une liste qui comporte toujours les terminaux VT100 ou VT220. Il existe de nombreuses versions de Telnet. Le Telnet **client** peut tourner sous système d'exploitation DOS, Windows ou Unix. Le Telnet **Serveur** (Telnet deamon = **telnetd)** tourne en général sous Unix. Au fur et à mesure que l'utilisateur tape les caractères au clavier, ils sont reçus par le serveur Telnet et transmis à Unix comme s'il s'agissait d'un terminal local en mode asynchrone connecté par une liaison série.

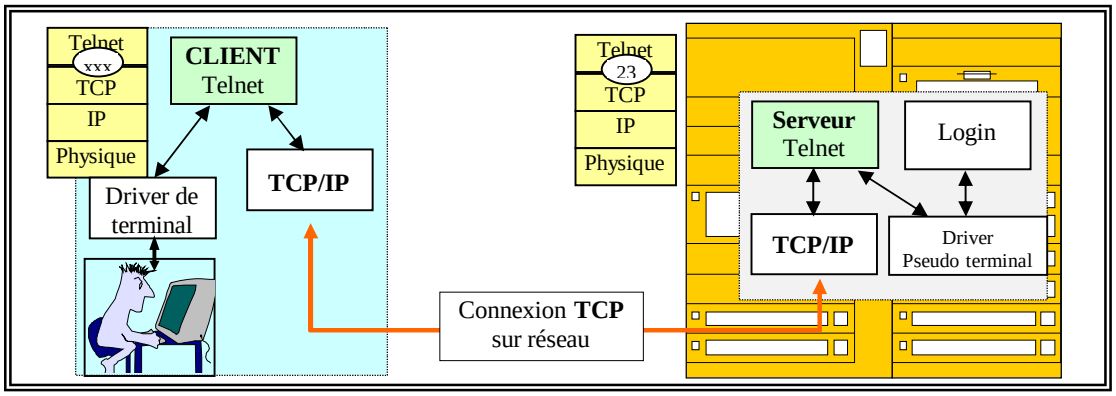


Figure : Telnet.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com


```
Last login: Fri Mar 14 15:22:59 from 126.0.1.121

Digital UNIX V4.0 (Rev. 386); Fri Nov  8 11:42:05 GMT+0100 1996

The installation software has successfully installed your system.

There are logfiles that contain a record of your installation.
These are:

        /var/adm/smlogs/install.cdf      - configuration description file
        /var/adm/smlogs/install.log      - general log file
        /var/adm/smlogs/install.FS.log   - file system creation logs
        /var/adm/smlogs/setld.log        - log for the setld(8) utility
        /var/adm/smlogs/fverify.log      - verification log file


% ls
backup          lprm.exe        mailer.exe      presentr.exe    resolvip.exe
bin             lwpcfg.exe      novasync.exe    prtgui.exe      user04
lpq.exe         lwpcfgd.exe     nvtsvc.exe      rapfiler.exe    windows
lpq000.exe      lwpcon.exe      nwunpack.exe    rarpd.exe
lpr.exe         lwptimer.exe    ping.exe        rcp.exe
```

Figure : Connexion à un serveur Telnet sous Unix .

WWW :

Le Wide World Web est l'ensemble des serveurs qui stockent des documents au format **HTML**[H] (et autres) sur Internet. Pour assurer le dialogue entre les clients Web (les navigateurs Web) et les serveurs, on utilise le protocole **HTTP**[H] qui s'appuie sur TCP et IP.

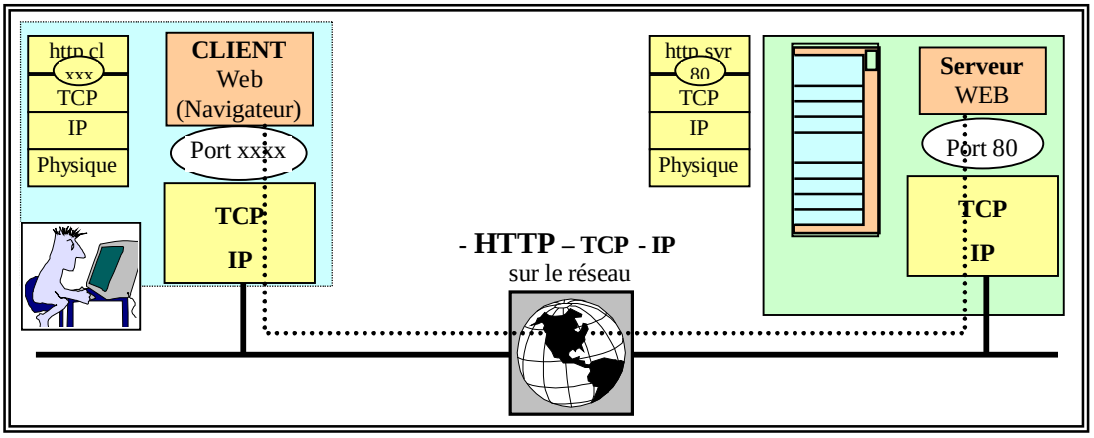


Figure 6-1 : Liaison WWW.

Les protocoles de messagerie SMTP, POP et IMAP4 :

La messagerie est un des services d'Internet les plus utilisés et les plus pratiques. Pl usieurs protocoles sont utilisés pour la transmission des messages.

SMTP

Le protocole SMTP permet d'envoyer les messages en ASCII vers le serveur du provider auquel on est raccordé

Lorsque l'utilisateur A veut envoyer un message, il le compose tout d'ab ord en utilisant un utilitaire de messager, (Outlook, Outlook Express, Message Composer, Eudora ou autre). Le message composé est d'abord envoyé vers une boîte d'envoi locale. Puis, le message est acheminé vers le serveur du provider à l'aide du protocole SMTP. Pour envoyer des messages non textuels (images, documents Word, programmes), on est obligé d'utiliser des utilitaires pour rendre la transmission compatible avec SMTP qui ne supporte que l'ASCII. Ces utilitaires sont UUENCODE / UUDECODE ou plus récem ment MIME[S].

HTML = Hypertext Markup Language
HTTP = Hypertext Transfer Protocol.
SMTP= Simple Mail Transfert Protocol.
Provider= Fournisseur de services Internet.
MIME= Multipurpose Internet Mail Extensions.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

POP et IMAP4

Le message est ensuite acheminé vers le serveur sur lequel est connecté le destinataire. Celui -ci n'étant pas forcément relié en permanence à ce serveur, il existe une boîte aux lettres personnelle dans laquelle seront stockés tous les messages non lus.

Le destinataire consulte sa boîte aux lettres et récupère ses messages grâce au protocole POP3 . Un protocole plus récent IMAP4 est parfois utilisé. Il possède l'avantage de permettre la consultation des messages sur le serveur sans forcement les rapatrier dans la station.

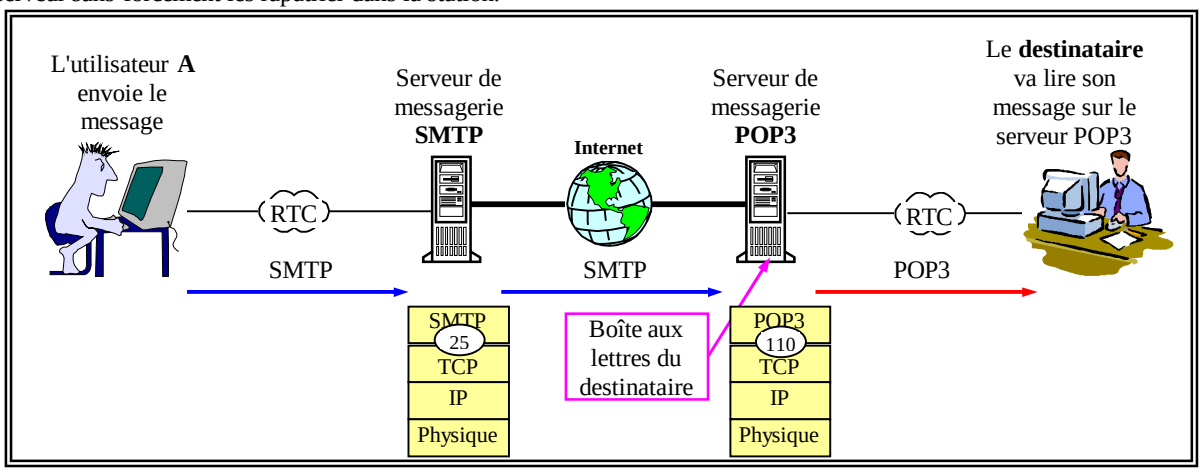


Figure : Messagerie Internet.

POP3= Post Office Protocol Version 3.
IMAP4= Internet Message Access Protocol Rev4.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

EXERCICE IV-1 :

1. Identifiez les classes d'adresses IP pour les réseaux suivants

210.23.67.102
66.23.148.0
158.23.251.33
144.23.117.254
192.254.23.123
144.207.78.1
63.125.23.211
192.25.128.36
128.12.254.98
134.223.156.89
127.0.0.1
224.23.108.23
223.78.27.144
77.123.28.167
191.249.222.234
19.23.12.255
188.67.76.235
134.255.123.22
143.52.213.212
207.22.45.219
117.117.117.117
193.23.255.77
199.23.255.7
145.2.229.252
238.23.177.8

2. Identification de host ID et du Network ID

Encerclez le Network ID de cette adresse: 1.102.45.177
Encerclez le Host ID de cette adresse: 196.22.177.13
Encerclez le Network ID de cette adresse: 133.156.55.102
Encerclez le Host ID de cette adresse: 221.252.77.10
Encerclez le Network ID de cette adresse: 123.12.45.77
Encerclez le Host ID de cette adresse: 126.252.77.103
Encerclez le Network ID de cette adresse: 13.1.255.102
Encerclez le Host ID de cette adresse: 171.242.177.109
Encerclez le Network ID de cette adresse: 193.156.155.192
Encerclez le Host ID de cette adresse: 21.52.177.188
Encerclez le Network ID de cette adresse: 77.77.45.77
Encerclez le Host ID de cette adresse: 191.252.77.13
Encerclez le Network ID de cette adresse: 191.15.155.2
Encerclez le Host ID de cette adresse: 221.252.117.254
Encerclez le Network ID de cette adresse: 203.10.233.1
Encerclez le Host ID de cette adresse: 191.2.227.19
Encerclez le Network ID de cette adresse: 23.156.1.92
Encerclez le Host ID de cette adresse: 121.2.199.88
Encerclez le Network ID de cette adresse: 202.27.189.177
Encerclez le Host ID de cette adresse: 177.222.177.28
Encerclez le Network ID de cette adresse: 198.215.67.233
Encerclez le Host ID de cette adresse: 128.252.17.24
Encerclez le Network ID de cette adresse: 212.199.19.29
Encerclez le Host ID de cette adresse: 159.255.17.218
Encerclez le Network ID de cette adresse: 155.25.169.133
Encerclez le Host ID de cette adresse: 191.255.217.227

3. Qu'est ce qui ne va pas avec ces adresses:

(Lorsqu'elles sont utilisées pour identifier des hôtes sur un réseau. Toutes ne sont pas invalides.)

Suggestion:
Identifiez la classe de l'adresse
Passez en revue les conventions d'adressage:
Nombre binaire converti à décimal valide

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Etendue de la Class A, B et C
Le Network ID ou Host ID ne peut pas être tous des 0 ou des 1 (en binaire).
245.12.33.102
123.123.123.123
199.23.107.255
199.23.107.0
156.266.12.103
99.0.0.12
153.0.0.0
153.0.0.255
191.23.255.255
33.255.255.0
12.0.0.0
12.255.255.255
12.0.0.255
127.0.0.1
127.23.109.122
0.23.12.122
192.12.255.102
191.105.0.0
203.123.45.255
204.0.23.198
224.56.204.112
223.255.255.254
126.0.0.1
177.45.123.255

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

EXERCICE IV-2 :

Segmentation de réseaux en sous-réseaux

(classes C et B)

Note
Le premier sous-réseau est le sous-réseau #0.

Problème 1
Supposons un réseau IP dont l'adresse est 194.170.25.0. Vous avez besoin d'au moins 20 sous -réseaux avec au moins 5 hôtes (disponibles) par sous-réseau.
Combien de bits devez-vous emprunter? _____ _____
Quel est le nombre de sous-réseau total dont vous disposez? _____
Combien d'hôtes par sous-réseau avez-vous? _____
Quel est le masque de sous-réseau? _____ _____
Donnez l'étendue des adresses hôtes disponibles sur les sous -réseaux #1, #5 et #15.
_____
_____
_____ _____

Problème 2
Supposons un réseau IP dont l'adresse est 192.52.0.0. Vous empruntez 4 bits pour créer des sous -réseaux.
Quel est le nombre de sous-réseau total dont vous disposez? _____
Combien d'hôtes par sous-réseau avez-vous? _____
Quel est le masque de sous-réseau? _____
Donnez l'étendue des adresses hôtes disponibles sur les sous -réseaux #1, #5 et #10.
_____ _____
_____
_____

Problème 3
Supposons un réseau IP dont l'adresse est 130.100.0.0. Vous empruntez 4 bits pour créer des sous -réseaux.
Quel est le nombre de sous-réseau total dont vous disposez? _____
Combien d'hôtes par sous-réseau avez-vous? _____
Quel est le masque de sous-réseau? _____
Donnez l'étendue des adresses hôtes disponibles sur les sous -réseaux #1, #5 et #10.
_____
_____
_____

Problème 4
Supposons un réseau IP dont l'adresse est 191.68.0.0. Vous empruntez 10 bits pour créer des sous -réseaux.
Quel est le nombre de sous-réseau total dont vous disposez? _____
Combien d'hôtes par sous-réseau avez-vous? _____ _
Quel est le masque de sous-réseau? _____
Donnez l'étendue des adresses hôtes disponibles sur les sous -réseaux #1, #264 et #986.
_____
_____ _____
_____

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

CONTROLE CONTINU N°2

SOIT LA CAPTURE DE TRAMES SUIVANTE :

1. Indiquez **l'adresse source** MAC en hexadécimal : _____

2. Indiquez **l'adresse source IP** en notation décimale point : _____

3. Quel est **le nom** du champ de l'en-tête Ethernet dont les octets (0800) sont entourés dans la représentation en Hexa de cette trame ? _____

4. Enumérez les points qui différencient UDP de TCP.

_____
_____
_____
_____

```
Packet Number : 47          10:05:26
Length : 95 bytes
ether: ==================== Ethernet Datalink Layer ====================
       Station: HUB BRIDGE ----> Broadcast
       Type: 0x0800 (IP)
   ip: ======================= Internet Protocol =======================
       Station:126.0.1.5 ---->255.255.255.255
       Protocol: UDP
       Version: 4
       Header Length (32 bit words): 5
       Precedence: Routine
              Normal Delay, Normal Throughput, Normal Reliability
       Total length: 77
       Identification:     0
       Fragmentation allowed, Last fragment
       Fragment Offset: 0
       Time to Live: 60  seconds
       Checksum: 0xFF9B(Valid)
  udp: ===================== User Datagram Protocol ====================
       Source Port: 0
       Destination Port: SNMPTRAP
       Length = 57
       Checksum: 0x0000(checksum not used)
 snmp: ============== Simple Network Management Protocol ==============
       Message: 45 bytes
       Version: Version-1 (0)
       Community: public
       TRAP-PDU: 30 bytes
       Enterprise:
             iso(1).org(3).dod(6).internet(1).private(4).enterprises(1)
             .171.7.3
       Agent Address: (Network #) 126 0 1 5
       (Node) 105-99-76-32-76-73
       Generic trap: warmStart(1)
       Time stamp: 0(00:00:00)
       Variable bindings list: 0 bytes
```

CAPTURE DE TRAME SNMP

5. L'adresse IP d'une station est : **133.214.95.63**
Le masque défini dans les nœuds est : **255.255.0.0**
Quelle est la classe de l'adresse IP ? :_____
Existe-t-il un sous-réseau ? OUI NON (Rayez la mention inutile)
Si OUI, quelle est l'adresse du sous -réseau ? : _____

6. L'adresse IP d'une station est : **197.214.95.65**
Le masque défini dans les nœuds est : **255.255.255.192**
Quelle est la classe de l'adresse IP ? :_____
Existe-t-il un sous réseau ? OUI NON (Rayez la mention inutile)
Si OUI, quelle est l'adresse du sous -réseau ? : _____

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

7. Pour des adresses IP en classe B,
Quel est le masque de sous réseau par défaut ? _____ _____
Quel est le masque pour avoir 16 sous -réseaux? _____ _____

8. A quoi sert le fichier **Hosts** dans une machine travaillant sous **IP** ?

_____
_____

9. Rôle des applications ou commandes suivantes :

Telnet : _____

FTP:_____

Rlogin_____ _____

10. Vous souhaitez obtenir des adresses IP de manière automatique pour les ordinateurs portables qui se connectent sur votre réseau. Vous installez:
un service :.....
sur un serveur avec un OS ……..... ou …….....

11. Vous souhaitez faire des correspondances entre des noms d'ordinateurs Internet et des adresses IP, vous installez un serveur ..…….....

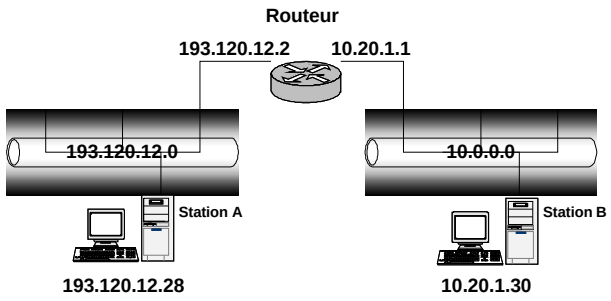
12. Soit l'adresse IP suivante exprimée en hexadécimal. Donnez sa valeur ne notion décimale pointée et en binaire.

Hex	**7E**	**0A**	**3B**	**25**
Déc. point				
Binaire				

13. A quoi sert l'adresse IP **127.0.0.1**?
.....…….
……

14. Quel est le rôle du protocole ARP ?
.....
.....

15. Soit l'inter-réseau suivant:



Quel est le nom du paramètre (à renseigner sur les stations) essentiel permettant la communication entre les stations A et B?
…….
Quelle est sa valeur pour la **station A**:……
Quelle est sa valeur pour la **station B**:……

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

V- LA TECHNOLOGIE DES SERVEURS RESEAUX

V-1- INTRODUCTION AUX SERVEURS RESEAUX

L'utilisation d'un réseau informatique dit lourd de type Windows NT / 2000 / 2003, Linux ou Novell Netware oblige l'utilisation d'un ou plusieurs ordinateur(s) central (aux). Ces ordinateurs peuvent être de tous types, y compris mainframe. Nous nous intéresserons ici aux serveurs réseaux de type PC X86. Un serveur peut-être un PC normal dans le cas d'un petit réseau et un serveur peut être ut ilisé comme station de travail de haut de gamme. Néanmoins, la majorité des serveurs sont des spécifiques. Les caractéristiques de ces ordinateurs doivent répondre à divers critères liés à la sécurités des données et des applications installées sur le serveur.
Avec l'évolution de l'informatique dans les entreprises, l'ordinateur central et l'installation périphérique devient primordial, le moindre arrêt de l'installation provoque immédiatement l'arrêt de l'usine avec les conséquences que l'on peut imaginer. Que cet arrêt soit de type problème logiciel, lié à un défaut de fonctionnement d'un serveur ou même à un switch récalcitrant est sans réelle importance. Le résultat est le même pour l'entreprise: perte de production, perte de données, ... Une installati on réseau **ne doit pas s'arrêter**. S'il a fait son travail de préparation des causes possibles de panne (et des solutions immédiates), un bon technicien de maintenance doit "se promener" dans l'usine. Le moindre arrêt, surtout s'il dure, se paye cash, autant minimiser les durées.
Avec le chapitre suivant, nous ferons un tour du côté des disques durs, de leurs types et de leurs regroupement (RAID). Néanmoins, les serveurs de grosses puissances ne se limitent pas à des disques durs ou des protections externes. L'architecture interne est également différente. Si un serveur ne doit jamais s'arrêter, il faut également que sa puissance soit suffisante pour l'application. Pour rappel, un serveur **ne doit pas fonctionner à plus de 10 % de charge en moyenne**, sous peine de ralentir l'application et les utilisateurs. Ceci n'entraîne pas forcément des serveurs musclés. Selon l'application, le nombre de PC connecté, la fonction du serveur (fichier, imprimante, programme), la configuration sera choisie en conséquence. Voyons les différentes solutions qui ont été adoptées pour (tenter) obtenir résultat.

V-2- SPECIFICITES EXTERNES

Les protection externes pour éviter l'arrêt d'un serveur par une main indélicate sont implantés sur les modèles de haute gamme.

- Blocage par clefs des boutons d'allumage, reset, accès au lecteur de disquette, ... bien que ceci n'est pas le plus important.
- Câbles de raccordement, doivent être fixés sur le boîtier ou dans un chemin de câble, pour éviter que les câbles ne s'arrachent par traction, ... Il doivent être étiquetés.

V-3- SPECIFICITES INTERNES

- disques durs rapides pour donner les informations le plus tôt possible après une requête d'un client connecté, si possible multi-sessions, ce qui implique des liaisons SCSI.
- sécurité des données en cas de "crash disk" (panne complète d'un disque dur): dédoublement des disques par systèmes RAID
- sécurité des données en cas de panne d'alimentation ou de baisse de tension: UPS
- sécurité des données en cas de panne complète d'un ordinateur (sauvegarde quotidienne)
- installation de disques, cartes électroniques "**à chaud**". Ceci signifie que le périphérique peut être remplacé alors que le PC continue de fonctionner.

En voyant la liste, ceci ne paraît pas trop compliqué. Evitons l'aspect externe. Ceci est lié au boîtie r d'une part et ... aux techniciens, administrateurs réseaux pour l'aspect câblage: pas de câblage à la va vite dans les passages. De plus, les salles informatiques conçues pour les serveurs réseaux sont généralement installées avec un faux plancher, ce qui permet de passer les câbles en-dessous et munies d'un système anti-feux avec des bonbonnes de gaz au fréon, un gaz inerte. Au prix d'une bonbonne,

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

évitez d'allumer votre cigarette dans ces salles. Ces salles sont généralement sous température de 18° contrôlées. Bref, cet aspect n'a pas grand chose à voir avec le cours, mais mieux vaut être au courant. Chaque serveur est connecté à un UPS, alimentation ininteruptible (onduleur). L'onduleur est de plus capable de contrôler le serveur (de l'éteindre) en cas de panne de courant ou de baisse de tension via un programme spécialisé. C'est également souvent le cas des HUBS et switch et périphériques externes annexes.
L'aspect interne est plus complexe. Les disques durs sont généralement de type SCSI. Ce type de liaison n'est guère plus performant en station que les disques durs E-IDE, sauf aux temps d'accès. Par contre, les liaisons SCSI sont plus performantes en multi-read. En cas de crash disque, on utilise des systèmes redondant des disques (RAID). On écrit les données sur chaque disques (de manière équivalente), mais on ne lit que sur un disque. En cas de crash, on continue sur le deuxième disque. En cas de crash complète d'un serveur, on peut coupler en permanence 2 serveurs de la même manière que les disques ci-dessus. Tous ces systèmes sont dits RAID. Pour les alimentations, on peut utiliser 2 alimentations couplées (on parle de dédoublées ou redondante). En cas de panne d'une, on continue sur l'autre. Chacune doit donc être ne mesure d'alimenter l'ensemble de manière autonome. Pour les cartes électroniques, le PCI 64 permet d'enlever ou d'insérer une carte sans couper la machine, à condition que le serveur soit installé avec un système d'exploitation compatible (par exemple Win2000). Le dédoublement de chaque partie d'une installation informatique pour garantir que si l'une tombe en panne, la deuxième partie prenne immédiatement la place s'appelle la **redondance des équipements**. Bref, il y a du boulot.
Au niveau des périphériques, nous en connaissons déjà quelques uns. Les bandes de sauvegarde sont pratiquement toujours utilisées, mais pas vraiment comme petite sauvegarde au cas où avec des vitesses de transfert qui n'ont rien à voir avec les bandes de types QIC de première année. De plus, on retrouve en externe des boîtiers contenant les disques durs par exemple, toujours en RAID.

V-4- CONFIGURATION DE BASE D'UN SERVEUR.

Avant de rentrer dans des solutions purement techniques, voyons un peu l'utilisation d'un serveur. Par définition, un serveur n'est pas une station de travail. Résultat, la carte graphique, le lecteur CD-ROM et le lecteur de disquette ne sont pas des composants primordiaux. L'écran ne doit pas non plus être un modèle multimédia de haute gamme. L'écran du serveur est généralement un 15" (voire un 14 noir et blanc) qui tourne "à vide". On ne s'intéresse à l'affichage que dans les cas critiques. Le lecteur CD-ROM n'est généralement pas non plus de type SCSI mais bien E-IDE, vu sa faible utilisation. Selon le système d'exploitation, on peut (ou on doit) le configurer via une station.
La mémoire doit quand à elle être suffisante, les disques de capacités doubles, voire triples par rapport à la capacité maximum que vous utiliserez sur cette machine. Je parle ici de la capacité effective, utilisable, sans rentrer dans la technologie RAID

V-5- MEMOIRE SERVEUR.

Première comparaisons avec les mémoires traditionnelles, les mémoires utilisées par les serveurs sont toutes de types utilisés dans les PC traditionnels. Les serveurs actuels utilisent des mémoire s **ECC** (Error Checking and Correcting ou Error Correction Code). Cette technologie utilise plusieurs bits de contrôle (parité) pour la vérification des données en mémoire. Ces mémoires sont auto-correctives. Cette mémoire peut détecter 4 erreurs et en corriger une sans arrêter le système. Un nouveau type de mémoires avec correction d'erreur AECC (Advanced Error Correcting Code) peut détecter 4 erreurs et en corriger 4 sans arrêter le système. Forcément, ces mécanismes ralentissent un peu le système.

V-6- PORTS INTERNES.

En bureautique, les ports courants sont PCI 32 bits et AGP. Ces ports ont deux problèmes. Le premier, ils ne sont pas déconnectables à chaud (**Hot plug**). Le remplacement d'une carte nécessite l'arrêt du serveur. Dans les petits serveurs, ceci ne pose pas de problèmes en pratiques. En effet, comme chaque fonction est exécutée par une seule carte, le serveur n'assure de toute façon plus sa fonction en cas de panne de carte. Par contre, dans les serveurs de haute gamme, toutes les cartes sont red ondantes. Une carte réseau est dédoublée. En cas de panne d'une carte, la fonction se poursuit sur la deuxième carte équivalente. Ceci permet de "réparer le serveur" sans l'arrêter.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Le deuxième problème de ces ports sont liés à la vitesse. Pour rappel, un port PCI bureautique est capable de transmettre 132 MB/s maximum sur l'ensemble des ports PCI (bande passante partagée). Vérifions par exemple une carte réseau en base 1000. Comme les liaisons réseau sont de type série, on peut diviser le taux de transfert par 10, ce qui nous fait 8 pour une seule carte réseau un taux de transfert de 100 MB/s. Vous pensez peut-être qu'il reste de la marche, mais ... les disques durs SCSI sont également connectés via une interface sur le port PCI. Prenons par exemple, une co nnexion disque dur Wide Ultra 3 SCSI (Ultra 160/m) qui est capable de transférer 160 MB/s: 100 MB/s + 160 MB/s =260 MB/s, largement supérieur aux 132 MB/s du port PCI 32 bits.
Tous les serveurs dignes de ce nom se doivent donc d'utiliser des bus internes p lus rapides. Développé conjointement par les principaux acteur de l'hardware informatique, les serveurs utilisent des liaisons PCI sur 64 bits (le taux de transfert est donc doublé). De plus, le port PCI commun utilise une vitesse de 33 Mhz. Les ports PCI-X vont jusqu'à 133 MHz. Ceci nous donne un taux de transfert de 132 MB/s * 2 (port 64 bits) * 4 (bus à 133 Mhz)= 1056 MB/s pour l'ensemble du bus PCI. Généralement, un serveur accepte également 1 ou 2 port PCI 32 bits (carte écran par exemple ou Ethernet 1 00 de réserve). Les ports 64 bits acceptent généralement uniquement les cartes 32 bits fonctionnant en 3,3 V. Pour reconnaître les ports 64 bits qui acceptent les cartes PC 32 bits, il suffit de vérifier s'il y a 2 encoches (uniquement cartes 3,3 V) ou 1 e ncoche (accepte les cartes 3.3 et 5V) dans la partie 32 bit du bus PCI 64 bits.

Avec les ports PCI-X, nous retrouvons les caractéristiques attendues: rapidité et Hot plu g (si le pilote de la carte le permet). Une dernière précision, ces cartes et l'implantation de ces bus sont chères. Chaque serveur n'inclue pas d'office un PCI-X à 133 Mhz. Il existe des cartes à 33, 66, 100 et 133 Mhz. En plus, de nombreux serveur n'incl uent pas un, mais 2 ou trois ports PCI-X séparés. Ceci permet également de supprimer les goulots.
Avec ces caractéristiques, un PC bureautique ne peut pas servir de serveur réseau.

V-7 PROCESSEUR SERVEUR.

Pour les caractéristiques effectives des processeu rs dédiés aux serveurs réseaux, vous pouvez vous référer à la page processeurs serveur. Cette partie ne reprend que les cas généraux.

Introduction

Le processeur d'un serveur n'est pas d'office une bête de compétition. Un serveur se fout généralement de traiter des applications multimédia. Sauf pour les serveurs de programmes, les processeurs sont généralement "faibles". Un serveur de Web peut à l'aise se contenter d'un Pentium III, voire d'un CELERON.
Par contre, dans les applications lourdes, les fabrican ts de processeurs se sont dirigés vers deux directions: les processeurs spécialisés et le multiprocesseur. Les deux sont en partie liés.
Les processeurs actuels sont 32 bits. Ceci signifie que les instructions en assembleur qu'ils lisent sont codées sur 32 bits. Avec les chauffards de l'informatique, pour augmenter les performances d'un processeur, vous pouvez soit augmenter la vitesse, soit doubler le nombre d'instructions par cycle d'horloge. Cette solution a déjà utilisée, mais les processeurs 64 bits ut ilisent cette possibilité différemment. En effet, comme les processeurs actuels, les programmes sont écrits en 32 bits . Un

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

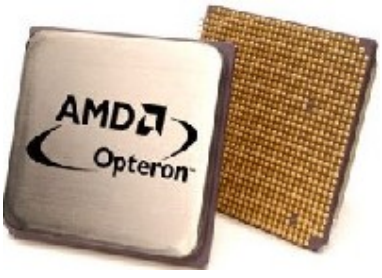
processeur 64 bits ne peut donc lire des instructions 32 bits et vis versa. INTEL avec son processeur 64 bits ITANIUM sorti en Juillet 2001 a contourné le problème en n'acceptant pas les anciennes instructions 32 bits (celle que nous connaissons). Ceci a nécessité de réécrire les programmes et systèmes d'exploitation ou plutôt de les recompiler, c'est à dire de reconvertir le programme assembleur 32 bits en 64 bits. Windows 64 bits existe pour ces processeurs, mais peu de programmes sont réellement sur le marché. Ceci réduit l'utilisation des Itanium à celle de serveur ou de station de très haute gamme. AMD a choisi le chemin inverse. Tout en créant un processeur 64 bits a gardé des compatibilités 32 bits. Les AMD 64 bits exécutent donc autant les applications actuelles que les applications 64 bits.
Une dernière chose, l'utilisation en bi-processeur et supérieur nécessite un système d'exploitation adapté. Windows NT, 2000 et XP Pro sont vendus de manière spécifiques. Novell oblige une option supplémentaire. UNIX - Linux est natif multi-processeurs, si la fonction est implantée en fonction de la carte mère / OS. Les versions "home" des systèmes d'exploitation Microsoft (Win95,98 Me et XP Home) ne gèrent pas le multi-processeur.

INTEL

Chez INTEL, les processeurs spécialisés 32 BITS sont de type XEON (plus l'ancien Pentium Pro). Par rapport aux Pentium normaux (Pentium III, Pentium IV), INTEL insère généralement des caches L1 et L2 plus importants. Pour parfaire le travail, le socket et les chipsets sont différents. Néanmoins, les Pentium III pourraient être utilisés en bi-processeur. Intel a supprimer cette possibilité de manière interne, mais pas dans la majorité des CELERON.
Les Itanium et Itanium II sont réservés aux réseaux exigeants puisqu'ils travaillent en 64 bits.
Remarque, ajouter un deuxième processeur (sur une carte mère qui l'accepte) nécessite un processeur de même vitesse et (en pratique) de même série de fabrication. Ceci n'est pas toujours facile à obtenir.
Une dernière remarque, avec les Pentium IV à 3.06 Ghz, INTEL inclue désormais, l'**hypertreading**. Cette technique permet d'émuler deux processeurs logiciels dans un seul Penti um. L'avantage serait lié à la vitesse mais les différents tests sont assez mitigés, notamment parce que l'application doit être dédiée à ce processus dans le cas de stations de travail. Par contre, cette fonction est largement implantée dans les ITANIUM et XEON.
Début 2004, INTEL annonce l'architecture NOCOMA pour les XEON. Ce processeur modifié est un processeur 32 bits capable d'exécuter certaines applications 64 bits. Il est donc comparable avec l'Opteron d'AMD et se positionne entre les XEON normaux et les ITANIUM Full 64 bits.

AMD

AMD produit depuis septembre 2001 des processeurs Athlon spécifiques capables de travailler en bi-processeurs, avec un chipset lui aussi spécifique. Ce sont les Athlons de type MP (multi-processeurs). L'opteron (version serveur de l'Athlon 64 bits) permettant d'utiliser jusqu'à 8 processeurs simultanément.



AMD développe 2 versions de son processeur 64 bits: l'Opteron et l'Athlon 64 bits. L'Opteron, sorti en avril 2003, est la version serveur – station informatique de haute gamme, au même titre que l'Itanium et son successeur l'Itanium II. L'Athlon 64 bits pour stations est sorti en septembre 2003. Pour rappel, ces processeurs sont également compatibles 32 bits et peuvent donc être utilisés avec des systèmes d'exploitation 32 bits habituels.
Les principales modifications par rapport à l'architecture K7 vient du nombre et de la taille des registres (les mémoires de travail internes) qui doivent supporter à la fois les nouvelles instructions AMD64 d'AMD et SSE d'INTEL.
Les Opteron sont gravés en 0,13 µ, tout comme les Athlons actuels, et utilisent un socket spécifique de type 940. Le cache L2 passe de 512K à 1 MB. La gestion mémoire n'est plus dévolue au chipset, mais bien directement au processeur qui gère 2 bancs (32 bits) de DD R333.
L'Opteron utilise 3 bus Hypertransports qui peuvent être reliés directement à un autre processeur (3,2 GB/s en bidirectionnel) soit à une puce gérant le PCI-X ou l'AGP.
Comme l'Opteron est dédié serveur, il est décliné sous 3 versions: 100, 200 et 80 0 qui disposent respectivement de 0, 1 et 3 bus processeurs pouvant être utilisés pour des machines utilisant 1,2 et 8

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

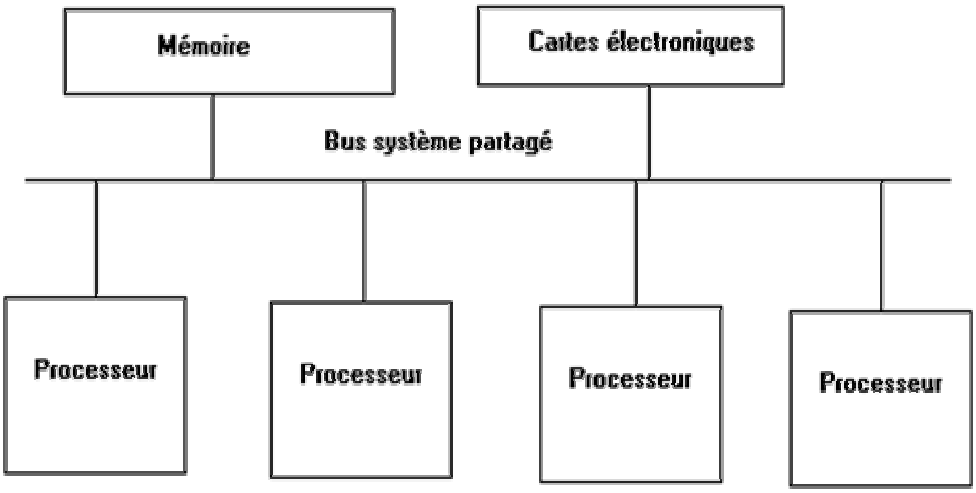
opteron. Chaque version est décliné en différentes vitesses. La version 200 est actuellement la seule disponible avec des vitesses de 1,4 , 1,6 et 1,8 Ghz.

V-8- LES TECHNIQUES MULTIPROCESSEURS.

Travailler avec plusieurs processeurs simultanément (dans la même machine) nécessite forcément une carte mère qui l'accepte. Le principe doit permettre de partager la mémoire, les accès disques et en règle générale tous les bus internes.
Deux techniques sont utilisées actuellement: le **SMP** à bus commuté (Symetric multiprocessing) et le multi-processing **Numa**. La différence entre les deux commencent à se réduire, tout simplement parce que les fabricants commencent à mélanger les deux, même si le principe de fonctionnement est différent.
Le SMP est surtout utilisé pour un petit nombre de processeurs, le Numa s'adapte mieux à un grand nombre de processeurs.

SMP, type UMA (Uniform Memory Access)

L'architecture **SMP** consiste à utiliser plusieurs processeurs partageant la même mémoire et les mêmes périphériques internes. Un seul système d'exploitation fait tourner l'ensembles des processeurs. A la suite de plusieurs avancées technologiques, les limites de ce p rincipe ont été repoussées. En effet, partager ne veut pas dire utilisation en même temps.



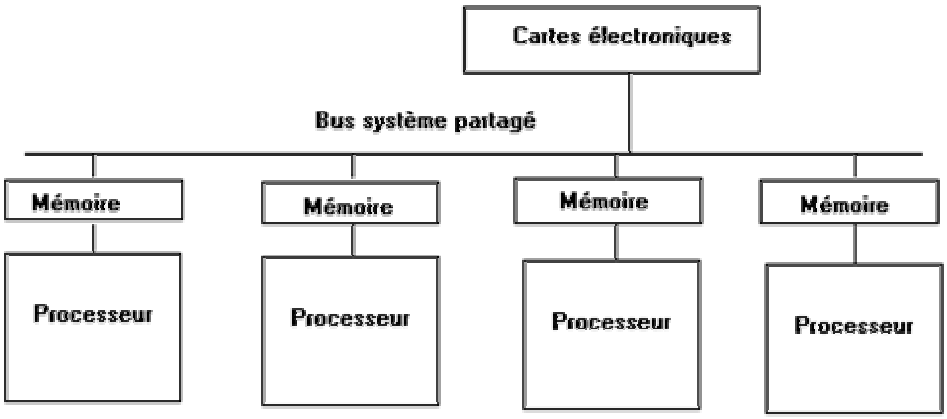
Architecture SMP type UMA

Le bus système a été longtemps le point faible du SMP. Ainsi, les premiers multi-processeurs faisaient communiquer les processeurs entre-eux par l'intermédiaire de bus systèmes partagés. Ceux-ci devenaient rapidement saturés au-delà de quelques processeurs. L'augmentation de la mémoire cache et l'augmentation de la fréquence de travail de ce bus ont permit d'améliorer les performances. Néanmoins, les possibilités d'évolution de ces bus sont faibles, la bande passante restant dans tous les cas constante.
Pour élaborer des plates-formes évolutives, les constructeurs de processeurs ont travaillé sur des architectures à bus commutés. Ceci a permit de créer des infrastructures d'interconnexion dont la bande passante pouvait être augmentée par paliers, grâce à des commutateurs supplémentaires. Ce type de connexion est à la base de systèmes modulaires. Les composants élémentaires ne sont plus les processeurs, mais des cartes filles bi ou quadri processeurs insérées dans des connecteurs sur une carte centrale de fond. C'est Sun qui a utilisé cette technique le premier av ec une machine capable d'exploiter jusque 64 microprocesseurs simultanément. La carte accueillant les cartes filles permet un débit de 12,8 GB/s et permet d'enficher jusque 16 cartes quadri -processeurs. Chaque ajout de cartes quadri-processeur voit l'ouverture de canaux d'interconnexion supplémentaire et donc une augmentation de la bande passante. Dans le système SUN, la mémoire est localisée sur chaque carte fille. Elle apparaît donc comme réservée par carte. En fait, tous les accès mémoire se fassent par par le bus central, que l'accès soit sur la même carte fille ou sur une autre. Par ce principe, la technique SUN

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

ressemble à une technique SMP. Chaque constructeur utilise actuellement une technique si pas identique, du moins équivalente. Certaines firmes ont néanmoins insérer un contrôleur local sur chaque carte fille.
Dans le monde PC, c'est INTEL (via des rachats) qui même le jeux. INTEL utilise un contrôleur de commutation de 2 bus d'accès mémoire, de 2 bus d'accès à des modules quadri -processeurs (le total est donc limité à deux cartes, soit 8 processeurs) et 1 bus d'entrées / sorties. Le tout est complété par des accélérateurs de cache.
Une autre solution, actuellement déployée par Unisys consiste à utiliser un système d'exploitation par processeur (architecture NUMA ci-dessous). Ceci permet actuellement d'utiliser jusqu'à 32 processeurs simultanément, en Windows 2000-NT, Netware ou UnixWare.

Multi-processing de type Numa (No Uniform memory access)



Architecture NUMA

L'architecture NUMA permet d'utiliser plus de processeurs. La technologie permet de regrouper des groupes de processeurs, utilisant leur propre mémoire locale, et de les relier entre -eux par des bus capable de délivrer plusieurs giga Octets par seconde. Par accès non uniforme à la mémoire, il faut comprendre ici qu'un processeur n'accédera pas dans les mêmes délais à une donnée en mémoire si celle-ci fait partie d'une mémoire locale ou distante. Cette différ ence de délais s'amenuise néanmoins, regroupant ainsi les architectures UMA et NUMA. La mémoire est par l'ensemble des processeurs. Ceci implique que le système NUMA exploite une gestion des cohérences de la mémoire cache capable de prendre en compte l'ens emble des processeurs attachés à la plate-forme.
La technologie multi-processeur ne s'appuie néanmoins pas uniquement sur la gestion des bus de connexion. Le communications sur les bus d'inter-connexion doivent également permettre de maximaliser le traitement des tâches entre les processeurs.
Une dernière remarque, et de taille, l'architecture NUMA oblige que chaque processeur fasse tourner son propre système d'exploitation, alors que dans le cas SMP, un seul système d'exploitation tourne pour l'ensemble des processeurs. **Ceci dédie donc NUMA pour des systèmes UNIX ou propriétaires et SMP pour le monde des serveurs INTEL – Windows**

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

VI- PREPARATION DU DISQUE DUR DU SERVEUR

VI-1- INTRODUCTION.

Les données (et son support principal, le disque dur) sont primordiales dans toutes applications informatiques. Dans le cas de serveurs, deux directions sont utilisées pour augmenter la vitesse et garantir la fiabilité en cas de panne d'un disque dur: l'utilisation de solutions SCSI pour le stockage et l'implantation du RAID. Les deux sont généralement implantés en même temps.

VI-2- TECHNOLOGIES SCSI.

Les connexions SCSI (Small Computer System Interface) ont par rapport aux périphériques IDE plusieurs avantages.

- Le **nombre de périphériques** connectés sur la même nappe est supérieur: jusque 15. L'adresse se fait par pontage ou sélecteur rotatif

- Une connexion SCSI est **multi-session**. En clair, le disque peut exécuter plusieurs applications en même temps (ou presque) et l'écriture (ou la lecture) d'un fichier ne doit pas attendre la fin de l'opération précédente. Ceci est le cas par exemple lorsque l'on écrit un gros fichier sur le disque dur, la lecture suivante ne doit pas attendre pour démarrer. Le SCSI est donc capable de gérer plusieurs requêtes de lecture /écriture en parallèle (jusque 255), au contraire de l'IDE qui ne peut traiter qu'une opération (complètement) à la fois. Ceci ne fonctionne de plus qu'avec un système d'exploitation compatible (Win NT, Win 2000 ou XP Pro, Novell), à l'exclusion de Win 95 et consort.

- Les périphériques SCSI peuvent être **internes ou externes**. Le transfert de données entre deux périphériques se fait directement par DMA entre les deux périphériques.

- Un disque dur SCSI inclut automatiquement un **contrôle d'erreur** des données enregistrées.

Tout ceci explique que les vitesses soient plus élevées qu'en IDE (même à taux de transfert équivalent), avec des prix qui varient en même temps.
La norme SCSI a évoluée, mais on rencontre encore quasiment toutes les normes selon les appareils à connecter. **NARROW** se réfère à un bus 8 bits, **WIDE** se réfère à un bus 16 bits.

Normes SCSI	Taux transfert MB/s maximum	Largeur bus (en bits)	Longueur maximum câble SCSI			Nombre conducteurs	Nb. max. connexion (non compris la carte contrôleur)
			SE	LVD	HVD		
SCSI (NARROW) SCSI 1	5	8	6 m	-	-	25	7
FAST NARROW SCSI	10	8	3 m	-	-	50	7
Fast Wide SCSI SCSI 2	20	16	3 m	12 m	25 m	68 ou 80	15
Ultra SCSI Narrow	20	8	3 m	-	-	50	3
Ultra SCSI Narrow	20	8	1,5 m	-	-	50	7
Wide Ultra SCSI SCSI 3	40	16 bits	3 m	-	-	68 ou 80	3
Wide Ultra SCSI	40	16 bits	1,50	-	-	68 ou 80	7

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Wide Ultra SCSISCSI 3 DIFFERENTIEL	40	16 bits	-	12 m	25 m	68 ou 80	15
Ultra 2 SCSI (Narrow)	40	8 bits	6 m	-	-	50	7
Wide Ultra 2 SCSI	80	16 bits	-	12 m	25 m	68 ou 80	15
Wide Ultra 160 Ultra 3 SCSI ou SCSI 5	160	16 bits	-	12 m	-	68 ou 80	15
Wide Ultra 320 SCSI	320	16 bits	-	12 m	-	68 ou 80	15
Par comparaison							
E-IDE ATA 133	133	16 bits	-	80 fils (connecteur 40)	2		

Le taux de transfert, la longueur des cordons, le nombre de fils et de périphériques diffèrent selon la norme.
Ce qu'il est important de connaître pour commander un cordon ou un terminateur :

. Le nombre de fils et le modèle des connecteurs.

. La norme SE, LVD ou HVD.

Tous les autres renseignements sont superflus sur le plan des connecteurs.
SCSI 1 (NARROW SCSI): Il est codé sur 8 bits seulement
SCSI 2 (WIDE SCSI) : Codé sur 16 bits il autorise un taux de transfert jusqu'à 20 MB/s

Carte SCSI 2 Adaptec AH 3940. Cette carte est identique à une 2940 mais possède 2 canaux internes distincts (RAID)

Connecteur SCSI2 interne

SCSI 3 (ULTRAWIDE SCSI) : il permet d'atteindre des taux de transfert de 40 MB/s

- SCSI 3 DIFFERENTIEL : il utilise du câble de très bonne qualité appairé et véhicule par paires deux signaux, le signal utile étant la différence entre les deux. Il existe 2 types de chaînes différentielles :
- **le HVD (High Voltage Differential)** qui travaille sous 5 volts et permet d'atteindre des longueurs de chaîne de 25 m alors que l'UltraWide ne permet pas de dépasser 6 m. Utilisé surtout dans des configurations professionnelles.
- **le LVD (Low Voltage Differential)** qui travaille sous 3,3 volts et permet d'atteindre 12 m de longueur de chaîne. Il utilise les nappes internes LVD, cordons LVD, terminateurs externes LVD et les terminateurs internes LVD.

La connectique est spécifique à chacune des 3 normes : les cordons et les nappes internes n'ont pas la même impédance en Ultra Wide, en HVD ou en LVD. Les terminateurs aussi sont différents. Il ne faut donc pas mélanger les différents types de cordons et terminateurs entre eux, surtout le HVD incompatible avec le reste. Toutefois la norme LVD permet de connecter des périphériques non LVD sur la carte hôte et à l'inverse de connecter des composants LVD sur une carte hôte non LVD. Bien entendu les débits ne seront pas dans ce cas ceux du LVD.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

La norme Ultra 2 SCSI LVD est une extension du SCSI 3. Sur le plan connectique les signaux sont véhiculés dans deux fils à la fois, le signal utile étant la différence entre les deux. Cette méthode est également utilisée en liaison Ethernet (entre autre). Les cordons LVD doivent de haute qualité et à la bonne impédance. La vitesse maximum théorique est de 80 MB/s.

La norme Ultra 3 SCSI ou Ultra 160/m ou SCSI 5 (SCSI PARALLEL INTERFACE SPI -3):
L'Ultra 160/m est une implantation spécifique de la norme Ultra 3 SCSI et ne retient que 3 éléments de cette norme :

. Taux de transfert doublé par rapport à l'Ultra 2 SCSI : 160 Mo/s au lieu de 80 Mo/s.

. Test physique du bus SCSI par le contrôleur, au démarrage, permettant de déterminer la vitesse de travail en fonction des différents éléments de la chaîne SCSI. Il va sans dire que la qualité des cordons et terminateurs jouera un rôle décisif dans la vitesse globale de la chaîne.

. Contrôle de redondance cyclique (CRC) qui permet le contrôle d'erreurs dans la transmission des données. Ce sont les caractéristiques essentielles qui caractérisent l'Ultra 160/m, le "/m" signifie que cette norme est manageable (test physique et CRC). La désignation utilisée pour l'Ultra 2 SCSI, LVD, est impropre car l'Ultra 3 SCSI est lui aussi LVD. Il utilise les mêmes connecteurs, donc cordons et terminateurs sont identiques, mais doivent être plus encore ici d'excellente qualité, compte tenu des débits très élevés. On peut aussi utiliser 15 périphériques sur une longueur totale de 12 m. Il est manageable car une carte Ultra 160/m saura gérer des périphériques connectés dans la même chaîne avec des vitesses différentes, en respectant leurs vitesses respectives : 80 Mo/s pour l'Ultra 2 SCSI ET 160 Mo/s pour le 160/m. Ainsi c'est la règle du maillon le plus faible qui détermine la vitesse globale de la chaîne disparaît. A l'inverse un contrôleur Ultra 2 SCSI pourra aussi gérer les 2 normes en même temps, mais à une vitesse unique de 80 Mo/s. Conclusion : totale compatibilité entre les 2 normes.

La norme Ultra 320 SCSI (SCSI PARALLEL INTERFACE SPI -4) :
Cette nouvelle norme enrichit tout en gardant les spécifications de la précédente norme Ultra 160/m :

- Transfert d'unités d'information (IU transfert ou packetization). Les informations indépendantes du flux de données, par exemple les commandes échangées entre la carte hôte et le disque dur, sont transférées à la vitesse nominale soit 320 Mo/s.

- Multiplexage des tâches d'entrées/sorties sans attendre la phase du BUS FREE. Continuité du flux de données sans phases d'inertie et exploitation optimisée des canaux disponibles. - La chaîne de commandes pour l'envoi d'un paquet de données se simplifie et les différentes étapes sont moins nombreuses, d'où une amélioration des taux de transferts.

- Rectification du signal de données par rapport au signal d'horloge (skew compensation). Skew est la différence de temps dans l'acheminement de deux signaux différents en provenance d'un même émetteur vers deux cibles différentes situées dans le même bus de traitement. Il peut s'agir d'une carte hôte émettant des signaux différents vers deux disques durs situés sur la même chaîne SCSI. Pour maintenir la logique du système, le délai entre les deux signaux est arbitré par un signal d'horloge. La vitesse de traitement est telle que tous les périphériques Ultra 320 accomplissent une compensation en mode réception car un écart d'une nanoseconde peut faire la différence entre un signal valide et une transmission incorrecte.

DB 25

Centronix 50 mâle externe (plus de pin que le connecteur centronix imprimante standard)

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

SUB 50 mâle

Connecteur DB68HD

VI-3- CONNEXION DE PERIPHERIQUES SCSI

Le choix du numéro de périphérique se fait soit par pontage, soit par un sélecteur rotatif. L'adresse doit être unique sur un même câble ou plutôt sur un même contrôleur. En effet, les périphériques internes et externes partagent généralement le même contrôleur.
La fin de la liaison des périphériques externes doit se terminer par une résistance de terminaison spécifique au type de connexion SCSI. En effet, pour les périphériques externes, la connexion est chaînée. On débute du contrôleur vers le périphérique. Le câble suivant passe du périphérique au périphérique suivant. Dans certains périphériques, la terminaison est inclue dans le périphériques (pontage à insérer pour l'activer).
Les câbles standard internes reprennent généralement seulement 3 connecteurs mais des modèles reprenant plus de périphériques se trouvent dans le commerce.
Généralement, on ne mélange pas les périphériques SCSI de différents types, néanmoins des terminaisons spéciales permettent de chaîner des périphériques NARROW (50 pin) avec des ULTRA WIDE (68 pin), tant en interne qu'en externe.

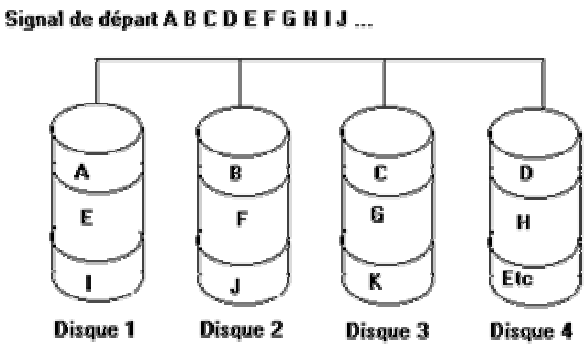
VI-4- RAID (REDUNDANT ARRAY OF INDEPENDANT DISK).

Cette possibilité nécessite un contrôleur disque particulier et ... toujours un système d'exploitation spécifique réseau lourd (une fois de plus, évitez Win 95 / 98). Adaptec fournis des contrôleurs RAID IDE, mais ce n'est pas la majorité des cas pour des questions de performances. Certains systèmes d'exploitation réseau permettent également, dans une moindre mesure, d'effectuer du **RAID logiciel**. Ceci n'est pas conseillé puisque c'est le processeur qui remplace le travail des contrôleurs, d'où un ralentissement.
Le RAID permet d'associer plusieurs unités de disques de même type (connexion SCSI et capacité) en une seule grappe. En cas de défaillance d'un disque, les versions de RAID autres que 0 permettent de reconstruire les données perdues à partir des autres unités de la grappe. L'implantation de cette technologie peut être de nature matérielle, logicielle ou passer par une combinaison des deux. Les solutions proposées peuvent être regroupées en six grandes familles, du Raid 0 au RAID 5.

RAID 0 (striping)

Le **RAID 0** n'apporte aucune sécurité des données, il augmente seulement le taux de transfert des informations. L'information est découpée à la suite de l'autre sur l'ensemble des disques durs (4 disques dans le cas ci-dessous mais plus généralement 2) L'unité qui regroupe les disques bénéficie de la somme des débits de chaque disque. Un accès (opération de le cture) ou un transfert (opération d'écriture) s'effectue en simultané sur l'ensemble de la grappe sur un mode parallèle. La panne d'un seul disque dur provoque la perte de toutes les données.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

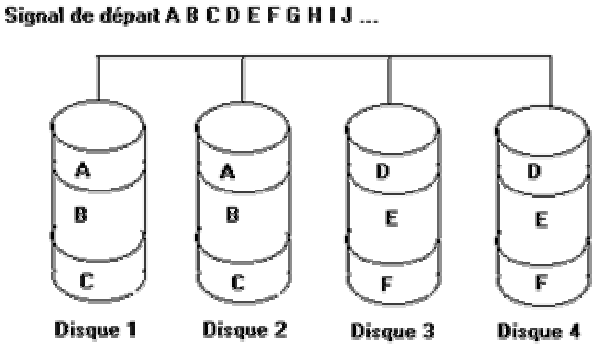


RAID 0

La capacité globale est équivalente à la somme des capacités de chaque disques durs (de capacités identiques).

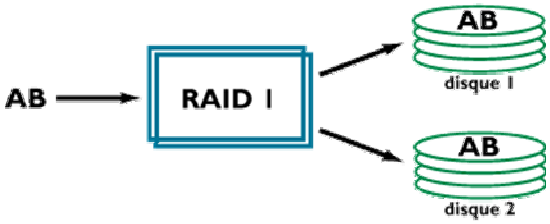
RAID 1 (Mirroring)

Dans les liaisons RAID 1, les données sont dupliquées intégralement sur un second disque ou sur un second groupe de disques durs. Les performances en lecture sont doublées grâce à l'accès simultané aux deux disques (à condition d'avoir deux contrôleurs séparés). Cette méthode réduit néanmoins la capacité de stockage. Il correspond au Mode logiciel "**Miroir**" de Windows NT4 ou Windows 2000 Server.

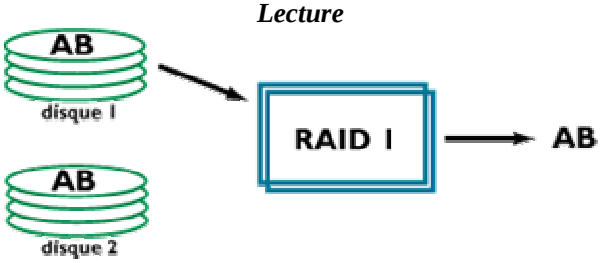


RAID 1

Ecriture



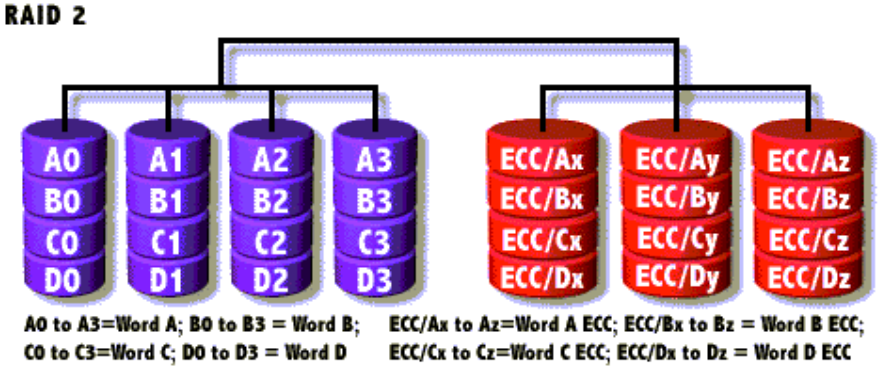
Lecture



Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

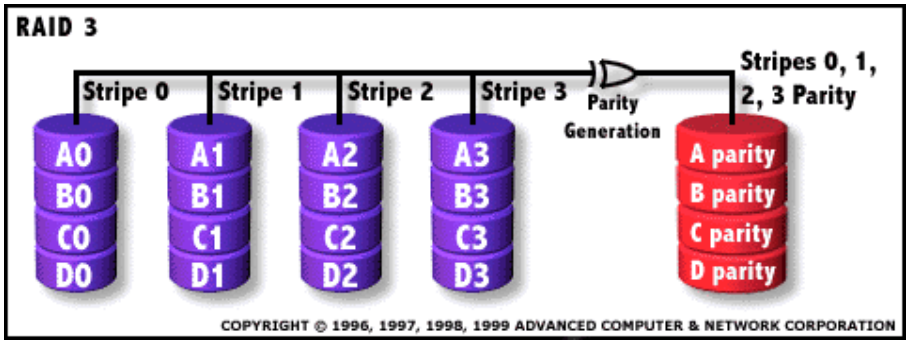
RAID 2

RAID 2 repose sur une grappe avec plusieurs disques de parité et une synchronisation des accès. Cette technologie est peu utilisée de par sa complexité et le surcoût qu'elle entraîne. Il est identique au RAID 0 avec un contrôle des données intégré. On utilise généralement 3 disques de contrôle pour 4 disques de données. La méthode de correction est l'ECC. Néanmoins, tous les disques durs SCSI incluent ce contrôle d'erreur, d'où le caractère anecdotique de ce mode. **Cette technologie n'as pas été commercialisée de manière industrielle.**



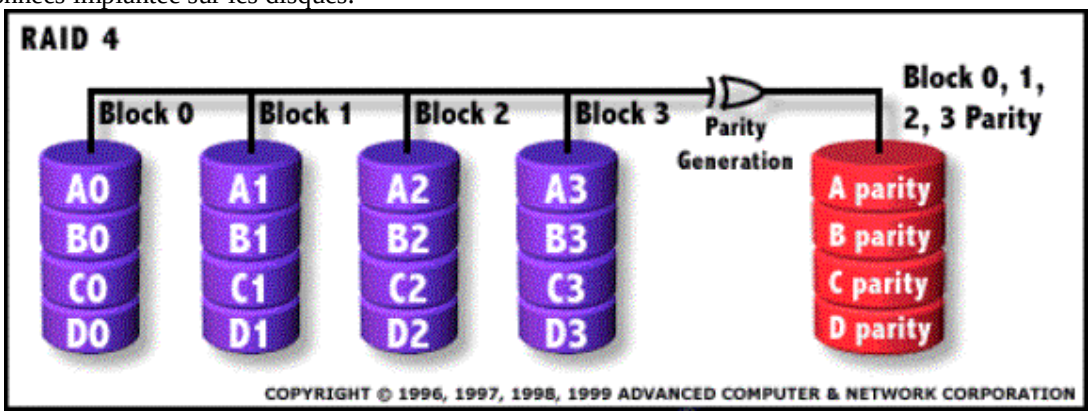
RAID 3

Le RAID 3 est basé sur des grappes de disques identiques avec une unité de stockage réservée au stockage du bit de parité. Si le disque de parité tombe en panne, on se retrouve en RAID 0. La sécurité des données est peu implantée. Attention, le disque de parité est 2 fois plus utilisé que les autres disques.



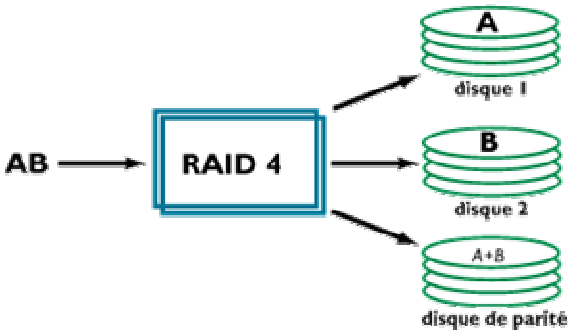
RAID 4

RAID 4 se différencie du RAID 3 par une gestion asynchrone des unités. Même si les accès fonctionnent en parallèle sur les différentes unités, le disque de parité est plus souvent sollicité. Ceci implique en RAID 3 un goulot d'étranglement. La seule différence avec le RAID 3 est la structure des données implantée sur les disques.

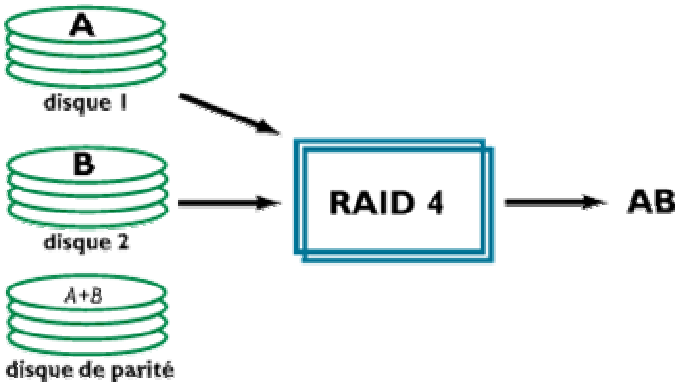


En **écriture**, les données sont décomposées en blocs de petite taille et répartis sur les différents disques composant le RAID 4. Simultanément, le contrôle de parité s'inscrit sur le disque dédié à cet effet.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com



Lecture :



Avantages :

- Tolérance de panne et parité centralisée sur un disque dédié.
- Parité : processus algorithmique permettant au systè me de reconstituer une donnée défectueuse ou manquante à partir de l'information de parité mémorisée au cours de l'écriture.
- Un sous-système en RAID 4 présente un rapport capacité/ performance/ investissement intéressant.
- Les performances en lecture des pi les de disques de niveau RAID 4 sont excellentes (comparables à celles du niveau RAID 0).
- Puisqu'il n'y a pas duplication des données, mais uniquement **enregistrement des données de parité correspondantes**, le coût par méga-octet d'une solution de niveau RAID mode 4 demeure raisonnable.

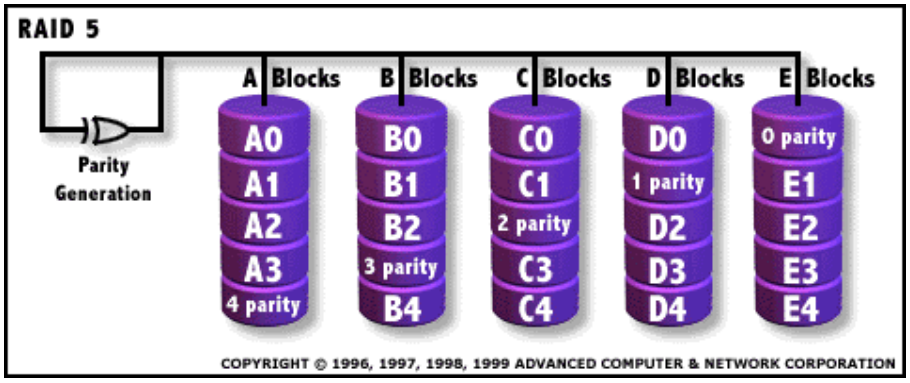
Inconvénients :

- Le défaut majeure provient de la **mise à jour** des données de parité qui **dégrade les performances** de Raid 4. Pour cette raison, le RAID 5 est toujours préférés aux systèmes RAID de niveau 4.

RAID 5

RAID 5 s'apparente au RAID 4 avec un bit de parité distribué sur l'ensemble des unités de la grappe, supprimant ainsi le fameux goulot d'étranglement tout en bénéficiant des performances de la gestion asynchrone. Ce mode correspond à l'agrégat par bandes avec parité so us NT4 ou 2000 Server. Les disques travaillent tous autant. Lors d'un échange à chaud (hot plug) d'un disque dur, les données sont recréées à partir des autres disques dur.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com



Avantages:

- Bonne tolérance aux erreurs
- Enormément d'implantations commerciales
- Hot-spare
- Hot-plug

Inconvénients:

- 3 disques au minimum
- En cas de problème, remise en ordre assez lente

Applications:

- Les applications qui utilisent les E/S de manière aléat oire sur de petits volumes
- Typiquement les serveurs de bases de données

Orthogonal RAID 5

L'Orthogonal RAID 5, technique logicielle développée par IBM, ce mode utilise un contrôleur par disque. Dans le langage courant, l'orthogonal RAID 5 est assimilé à u n RAID 5.

Les autres RAID

D'autres système RAID sont proposés. Ce ne sont que des RAID 5 évolués. Ces modes restent rares du fait d'une architecture complexe et un coût élevé.

- **RAID 6** est une extension du RAID 5 mais utilise une double parité. Ce système p ermet de travailler avec 2 disques durs défectueux, avec forcément une perte de performances.
- **RAID 7** met en jeux plusieurs disques de données couplé avec 1 ou plusieurs disques de parité. le contrôle des données et de la mémoire cache et le calcul de la pa rité se fait par un microcontrôleur. Ceci donne des performances jusque 50 % plus rapides que dans les autres modes RAID. Cette solution est une marque déposée de Storage Computer Corporation
- **RAID 10** implante le striping (RAID 0) couplé au Mirroring (RAID 1). Une excellente mais coûteuse solution de tolérance de panne. Ce système est le plus sûr et le plus rapide. Néanmoins, sa difficulté de mise en oeuvre et le prix le rendent peu utilisé.

VI-5- RAID HARDWARE ET SOFTWARE.

Le RAID peut être géré de manière hardware ou logiciel. La gamme des systèmes d'exploitation "professionnels" de Microsoft peuvent gérer le RAID de manière logicielle: Windows NT, 2000 en version serveur gèrent le RAID 0, 1, 5
Netware gère en mode natif (logiciel) le RAID 1

- Linux gère les RAID 0, 1, 4 et 5
- Les séries "amateurs" (DOS, WIN95/98/Me et XP Home) ne gèrent pas le RAID en mode natif.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Cette manière de procéder permet au système d'exploitation d'utiliser plusieurs disques en mode RAID sans hardware dédié. Par contre, en utilisant un hardware (avec le pilote associé) adéquat, **tous les systèmes d'exploitation peuvent travailler en RAID en théorie**. Pour rappel, les systèmes d'exploitation "amateurs" de Microsoft ne tirent pas non plus partie des possibilités de l'SCSI, notamment pour le transfert par DMA simultané de données entres disques durs.

VI-6- SOLUTIONS RAID HARDWARE.

Voici quelques solutions de contrôleur RAID matériels.

Adaptec AAA-132

Carte RAID SCSI Adaptec AAA-132 (2 canaux W). Remarquez en haut les quatre connecteurs (2 wide sur 16 bits et deux narrow sur 8 bits) et sur la droite le connecteur wide 16 bits externe. En bas à gauche, un emplacement pour de la mémoire cache (ici occupé p ar une barrette mémoire Simm de 70 pins).

ADAPTEC ATA RAID 2400 A

Carte RAID ATA/100 complète et abordable pour la sécurité des données. Idéale pour les utilisateurs qui souhaitent bénéficier de fonctions RAID avancées avec des disques durs ATA (de type ID E).
La carte 2400A est une solution RAID à coprocesseur pour les environnements de serveurs utilisant des disques ATA-100. Elle prend en charge jusqu'à 4 disques avec des taux de transferts atteignant 100 Mo/s par canal sur 4 canaux - pour une fonctionnalité RAID de niveau supérieur à un prix abordable. C'est la solution idéale pour augmenter la capacité et les performances du serveur. Des fonctions d'administration évoluées sont proposées par le logiciel Storage Manager Pro d'Adaptec.

Principales caractéristiques

- Coprocesseur i960RS
- Mémoire extensible jusqu'à 128 Mo
- 4 canaux pour 4 disques max.
- RAID 0, 1, 0/1, 5, JBOD
- Interface graphique évoluée
- Extension de capacité en ligne
- Remplacement automatique, Immédiat

D'autres modèles et marques existent en IDE ou en SCSI. Les nouvelles cartes mères intègrent cette fonction en SATA

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

VI-7- PARTITIONS DE DISQUES

Type de partitions

Il existe trois sortes de partitions :

- **les partitions principales (ou primaires)** : Dans tout système DOS/Windows, il faut absolument avoir au moins une partition principal qui contiendra le système. Cette partition devra ensuite être activée, puis formatée. Par défaut la lettre C représente cette partition, on l'appelle aussi la partition bootable.

- **les partitions étendues** : Les systèmes DOS/Win9x ne peuvent en avoir qu'une seule. Une partition étendue peut contenir un ou plusieurs lecteurs logiques.

- **les lecteurs logiques** : Un lecteur logique est toujours identifié par une lettre. Une fois créé, chaque lecteur logique devra être formaté avant d'être utilisé.

- **les partitions non DOS** : Ce type de partition ne peut pas être créée avec fdisk. On les utilise généralement pour l'installation d'autres systèmes d'exploitation (Linux, NT, OS/2, etc.). Si on prévoit avoir besoin d'un autre système d'exploitation, il suffit de laisser un espace libre sur le disque.

Identification des partitions

Connecteur IDE	Périphérique IDE	Windows (98/XP)	Linux – Accès
IDE 0 Master	1er disque dur	-	/dev/hda
	1ière part. princ. active	C:\	/dev/hda1-- /mnt/win_c
	Part. étendue	-	/dev/hda2
	1er lecteur logique	E:\	/dev/hda5 -- /mnt/win_e
	2ième lecteur logique	F:\	/dev/hda6
IDE 0 Slave	CD-ROM	H :\	/dev/hdb -- /mnt/cdrom
IDE 1 Master	2ième disque dur	-	/dev/hdc
	1ière part. princ.	D :\	/dev/hdc1 -- /mnt/win_d
	1er lecteur logique	G:\	/dev/hdc5 -- /mnt/win_g

Note : Ce qu'il faut savoir sur l'affectation des lettres sous Windows :

- les disques durs passent avant les lecteurs de cd-rom, graveurs de cd-rom, lecteurs zip.
- les partitions primaires des disques durs passent avant les partitions logiques.
- on peut définir la lettre d'un lecteur de cd-rom ou d'un graveur de cd-rom

Systèmes de fichiers (aperçu)

- FAT :
- VFAT :
- FAT32 :
- NTFS :
- EXT2 :
- EXT3 :

Outils de partitionnement des disques

FDISK (win98, winXP, Linux) :

Fdisk est présent sur toutes les disquettes d'amorce des différents systèmes. Attention ! Il existe différentes versions de ce programme, chacune étant associée à un système d'exploitation. Ainsi on aura des fdisk différents et incompatibles pour : DOS, Windows 95, Windows 98 et même Linux.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

. **Pour lancer le programme** :
...>fdisk

. **Menu principal de Fdisk** :

1. Création d'une partition ou unité logique

2. Activation d'une partition :

Pour activer la partition principale, afin de pouvoir booter un système dessus. Par défaut, la partition
principale porte le numéro 1 et est précédée par la lettre C.

3. Suppression d'une partition ou unité logique :

Ici, il est préférable de savoir ce qu'on fait. Car toute suppression de partition ou lecteur logique détruira les
données qu'ils contiennent. On ne peut pas supprimer avec cette option :
- la partition principale s'il reste des partitions étendues
- une partition non DOS (NTFS par exemple…)
- une partition étendue qui contient encore des lecteurs logiques.

4. Affichage des informations sur les partitions :

Ce n'est pas dangereux et ça donne une idée de ce qu'est une partition principale vs un lecteur logique.

5. Sélection d'un autre lecteur de disque dur

. **La commande fdisk /mbr** :

Cette commande sert UNIQUEMENT à restaurer le programme situé dans le Master Boot Record du disque de démarrage (et lui seul, défini dans la configuration du BIOS). Ce programme de 442 octets, situé au début de ce secteur, avant la table de partition, sert à dé terminer la partition active à partir de cette table et à charger le secteur de boot de cette partition.

Master Boot Record. Le premier secteur absolu sur un Disque Dur de PC : tête 0, piste 0, secteur 1 (parfois 0 lui aussi). Il contient la table des P artitions ou un simple Boot

Delpart :

Delpart est un utilitaire très pratique pour supprimer des partitions (notamment des partitions non -dos comme NTFS), impossibles à supprimer avec Fdisk : http://www.aidewindows.net/pratique/delpart.zip

Partition Magic :

FreeFDISK :

On peut utiliser **Free FDISK** à la place de l'utilitaire Microsoft. Il est entièrement compatible avec le FDISK traditionnel de MS, mais il fait plein d'autres choses, et documen tées (à la différence de l'outil MS). En particulier, un truc tout bête mais drôlement IMPORTANT : il permet de sauvegarder/restaurer le MBR."
Télécharger FreeFDISK : http://ffdisk.webaps.de/fdisk101.zip

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

VII- LES OUTILS D'ADMINISTRATION RESEAUX ET LEURS CARACTERISTIQUES PRINCIPALES

L'administration des réseaux est un outil indispensable qu'il faut prendre en compte avec beaucoup de sérieux lorsque l'on a décidé de s'investir dans la conception d'un réseau. L e travail de l'administrateur n'est pas du tout repos et il se trouve malheureusement que c'est un métier occulte très ingrat. En effet, lorsque le travail est bien fait, alors, c'est le gestionnaire qui est bien content car on ne voit jamais l'impact de la logistique informatique derrière qui a permis de rendre possible et fiable les objectifs atteints. Par contre, vous vous rendrez compte immédiatement que dès que le réseau marque des signes d'essoufflement, les gestionnaires s'en prennent à l'administrat eur du réseau informatique, et ce, quelque soit les loyaux services rendus de par le passé. Mais c'est toujours ainsi et dans pratiquement tous les domaines. Mais ceci étant, c'est un très beau métier dont les expériences sont toujours très enrichissantes. L'administrateur réseau, qui se doit d'être très intègre, a à sa charge la gestion du réseau informatique. C'est une charge tellement importante que l'ISO (International Standard Organization) a dû définir cinq (5) directives pour spécifier l'étendu du tr avail d'administration. Ainsi, l'administrateur réseau se doit de :

Surveiller et réparer les anomalies comme un câble défectueux ou autre…
S'occuper de toutes les configurations, que ce soit sur les postes ou sur les éléments du réseau.
Gérer toute la sécurité du réseau (mots de passe, coupes-feux…).
Mesurer et analyser les performances du réseau.
Gérer les informations comptables du réseau (coût des liaisons longues distances, etc…).

Vous pourrez penser que c'est en grande partie le travail d'un technic ien de maintenance. Mais il se trouve que tout a évolué et qu'aujourd'hui, on ne peut pas concevoir dans ce domaine un administrateur réseau qui ne puisse pas maîtriser le logiciel et le matériel ! Mais rassurez-vous, pour une bonne partie de cette tâche, des logiciels d'administration de réseau aideront l'administrateur. Mais, il ne suffit pas de posséder tous les outils d'administrations réseau, il faut que l'administrateur réseau développe son inspiration, la perception de son réseau, son intuition. Ce s ont tous ces éléments qui pourront l'aider dans ce métier. Pour vous donner un exemple : un petit champ magnétique peut vous rendre « fou » un réseau. Si l'administrateur réseau n'a pas cette notion, il cherchera très longtemps la cause de la perturbation avec peu de chance de tomber sur la bonne ! De plus, il ne s'agit pas tout simplement de déceler les anomalies, il faut savoir le faire très rapidement… au goût des exploitants ! La maîtrise de « pouvoir penser réseau » est capitale pour un administrateur réseau qui veut avoir la capacité de contrôler son réseau, de l'optimiser et de savoir le faire évoluer. Il faut qu'il sache tâter l'état de santé de son réseau.

On peut conclure cette introduction en définissant l'administration réseau comme étant le con trôle des données d'un réseau complexe de manière à en optimiser le fonctionnement et les performances. Les outils d'administration étant les instruments de l'administrateur réseau pour réussir cette mission. Vous constaterez que cette étude concerne l'adm inistration globale des réseaux. Il y sera ainsi question des protocoles, des bases de données d'administration, etc. Les systèmes d'exploitation de réseaux ne seront pas traités ici.

VII-1- LES SPECIFICATIONS TECHNIQUES CONTRACTUELLES

Avant éviter de se lancer corps et âme dans la conception d'un réseau, il faut éviter d'oublier les préalables : le cahier des charges. On ne se lance pas dans la mise en œuvre d'un réseau sans plan de bataille. Il faut savoir dimensionner son réseau, déterminer le trafic q ui y transitera, la bande passante, les différents supports, les différentes ressources en mettre en jeu, l'objectif du réseau, les différentes topologies, quelle philosophie adopter, etc… Il faut repérer ce que vous apportera b plus un réseau par rapport au moment il était inexistant afin d'être assurer que les investissements valent la chandelle.

Pour déterminer les spécifications techniques pour un réseau, il faut élaborer un catalogue (non exhaustif) des services d'assistance que le service informati que peut mettre en œuvre selon les besoins actuels de l'institution Il faut donc procéder à une analyse profonde des besoins puis les structurer. Il

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

faut donc que la suite des travaux se fassent sur la base des documents complets et précis afin d'éviter tout malentendu, ce qui aura pour conséquences de minimiser les retards dans l'exécution des tavaux.

Etant donné que l'informatique permet d'automatiser les tâches répétitives, d'améliorer la communication entre collaborateurs, de professionnaliser la commu nication clients/fournisseurs et d'aider à prendre les décisions importantes, il faudra arriver à intégrer ces opportunités dans une stratégie d'entreprise afin de pouvoir faire face aux grands défis de la société de l'information, du commerce électronique et de la mondialisation économique.

De nos jours, une coopération efficace est fondée sur l'utilisation rationnelle d'un réseau informatique. Ce réseau vous permettra de partager efficacement informations, fax, et imprimantes. Il peut également vous aider à stimuler la communication interne et à sécuriser vos documents (bases de données, comptabilité,…).

L'utilisation d'un logiciel afin de pouvoir « définir » la configuration et suivre la construction du réseau, nécessitent des compétences spécifiques sa ns lesquelles il vous sera difficile d'assurer la qualité de tels projets.

L'interconnexion à l'Internet ouvrira de nouveaux horizons à votre réseau. Cependant, parallèlement à ces avantages se pose le problème de la sécurité de votre système d'informatio n. Il faudra ainsi prévoir tous les outils nécessaires à l'administration quotidienne du réseau avant de subir les dégâts d'une intrusion, d'un virus ou d'une destruction accidentelle des données.

Installer un réseau informatique peut vous aider à stimule r la communication inter-utilisateurs. Le groupware en permettra l'optimisation. En effet, rassemblant divers outils de communication (agenda partagé, mail,…), le groupware dynamisera la circulation de l'information et développera les collaborations au sei n de vos utilisateurs.

VII-2- Les solutions d'administration

Nous allons commencer par étudier l'évolution des protocoles afin de mieux comprendre la raison d'être des standards actuels en matière d'administration réseau. Depuis l'avènement de l'ARPANET en 1969, les petits réseaux informatiques isolés évoluèrent vers des grands réseaux interconnectés pour donner naissance à l'Internet. La gestion de ces petits réseaux devenait alors de plus en plus compliqué. Aussi, le développement d'un protocole spécifiq ue d'administration réseau s'avéra alors nécessaire.

En 1988, l'Internet Activities Board (IAB) approuva le développement de deux (2) protocoles : le SNMP (Simple Network Management Protocol) et de CMOT (Common Management Information Protocol Over TCP/IP) avec l'idée que le SNMP fut une solution à court terme, la préférence étant marquée pour le CMIP.

CMOT est dérivé de CMIP (Common Management Information Protocol) qui a été prévu pour être exploité sur OSI. Afin de faciliter la transition future de SNMP vers CMOT (CMIP over TCP/IP), et en attendant que OSI puisse émerger pour que l'on puisse reléguer le TCP/IP (!) aux oubliettes, ... il a été décidé de développer CMOT dans une phase purement transitoire. Afin de s'assurer que CMIP sera bel et bien le standard en matière d'administration réseau, l'IAB imposa le ***modèle informationnel*** défini par l'OSI. Ainsi, CMOT et SNMP doivent utiliser une même base de données d'objets gérables appelée MIB (Management Information Base). Donc, une SMI (Structure of Managed Information) et une MIB (Management Information Protocol) communes devaient être définies et utilisées. Il est « *malheureusement* » vite apparu que cette contrainte était non réaliste car en SNMP, on manipule essentiellement des variables et en CMIP, on ma nipule des objets au sens de la technologie orientée objet.

En 1989, l'IAB est revenu sur sa décision en acceptant que les deux protocoles suivent une évolution parallèle et indépendante. Et une fois libéré de la contrainte de compatibilité avec OSI, les progrès ont été rapides. Le malheur des uns faisant le bonheur des autres, SNMP a été adopté par de nombreux constructeurs et est devenu à ce jour un standard très répandu de gestion réseau. Une des raisons

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

supplémentaires qui a fait que les constructeurs aient opté pour cet agent, c'est qu'un agent SNMP occupe moins de 10 ko de mémoire au sein d'un équipement alors qu'un agent CMIP en requiert près d'une centaine de ko.

La MIB, organisée selon une arborescence hiérarchique appelé MIT (Management Informati on Tree), détient toutes les informations des équipements à administrer se trouvant dans le réseau. Ces équipements sont repérés par une clé unique et sera gérée comme telle par un petit programme d'administration réseau appelé agent. C'est cet agent qui s era responsable pour faire parvenir à la plate-forme d'administration toutes les informations concernant l'équipement qu'il représente. Bien entendu, cet agent ne fait pas de zèle, il attend calmement que les requêtes soient formulées par la plate-forme d'administration. Pour lui permettre à la MIB d'élargir le champs de travail de l'administrateur, notamment ce qui concerne les routeurs et les ponts, un second standard fut défini par rajouter d'objets supplémentaires dans quelques unes des catégories de la MIB initiale, alors redéfinie MIB I. Ce standard est appelé MIB II et, fort de près de 180 objets, a remplacé la MIB I dans l'arborescence du MIT. Ainsi, la MIB RMON (Remote Monitoring) fait partie de l'arborescence et elle offre des fonctions proches de celles des analyseurs de réseaux.

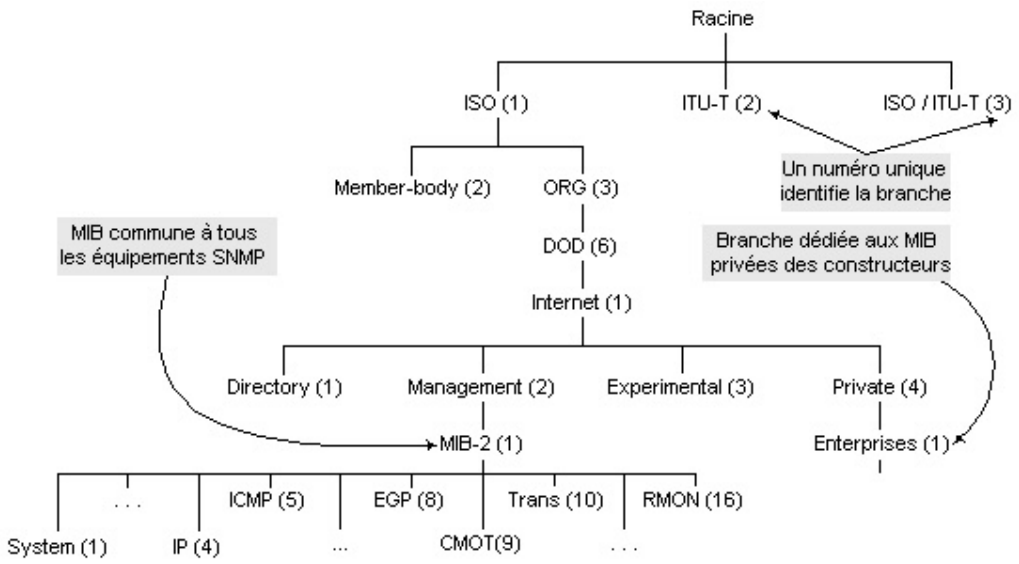


Figure : Extrait d'arborescence de la MIB

Une MIB est donc simplement une collection d'informations concernant tous les objets qui sont sous la responsabilité d'un agent donné. Ces informations sont codifiées dans le MIT selon le standard ASN.1 (Abstract Syntax Number 1). A partir de ce codage, il est alors assez simple de déterminer et de représenter l'identificateur d'un objet (Object IDentifier ou OID) dans le MIT.

Afin d'avoir une idée plus claire du codage ASN.1 au sein du MIT, nous pouvons voir que l'identificateur d'un objet d'administration commencera par ***1.3.6.1.2*** (***iso.org.dod.internet.management***), tandis l'identificateur d'un objet appartenant à un constructeur commencera par ***1.3.6.1.4.1*** (***iso.org.dod.internet.private.enterprises***). C'est aussi simple que çà !

Les protocoles liés à l'administration

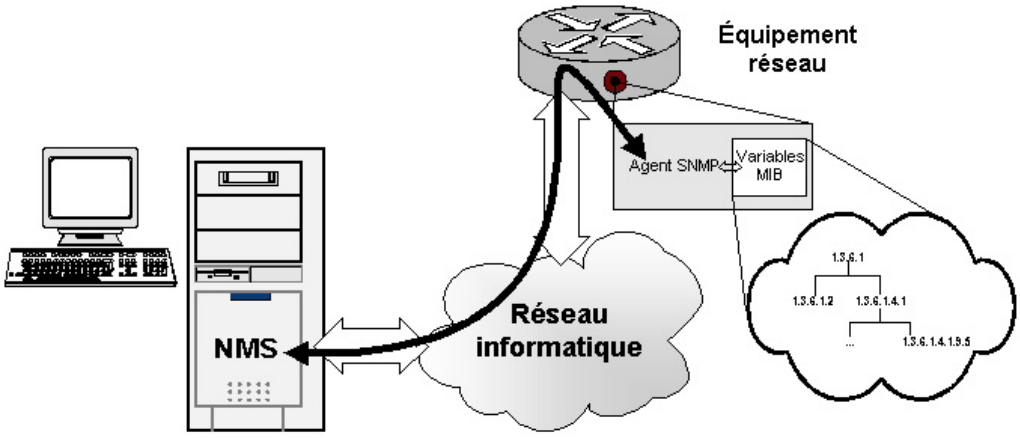
Le SNMP

SNMP (Simple Network Management Protocol) est un protocole de gestion de réseau. C'est actuellement le protocole standard pour l'administration de réseau. I l part du principe qu'un système d'administration réseau se compose :

- de nœuds administrés (MN = Managed Node) chacun contenant un agent. Les agents sont les ***serveurs***.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

- d'au moins une station d'administration. (NMS = Network Management Station). Cette station d'administration est le ***Client***;
- d'un protocole réseau utilisé par la NMS et les agents pour échanger des informations d'administration.(ici ***SNMP***).



Nous constatons que nous sommes en présence d'un modèle Client/Serveur mis à part le fait que le schéma est inhabituel puisqu'il y a un client et beaucoup de serveurs. Comme explicité plus haut, le client est en réalité la plate-forme d'administration tandis que les serveurs sont tous agents SNMP des équipements réseau (cf. schéma ci-dessus). Il y aura autant de serveurs que d'équipements réseau dotés d'agent SNMP.
SNMP utilise les SMIs pour donner l'ensemble des règles de définition des objets à gérer et les MIBs pour représenter la base de données de l'ensemble des objets pour un agent donné. La statio n d'administration lit les informations de l'agent et en agissant, sur ce dernier, modifie la valeur de certains objets.
L'architecture des couches réseaux selon le modèle OSI sur lesquelles s'appuient SNMP est la suivante:

<table>
<tr><th colspan="2">Modèle OSI</th><th>Modèle TCP/IP (proto cole)</th></tr>
<tr><td>7</td><td>Application</td><td rowspan="3">SNMP</td></tr>
<tr><td>6</td><td>Présentation</td></tr>
<tr><td>5</td><td>Session</td></tr>
<tr><td>4</td><td>Transport</td><td>UDP</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Réseau</td><td>IP</td></tr>
<tr><td rowspan="3">Interface réseau</td></tr>
<tr><td>2</td><td>Liaison</td></tr>
<tr><td>1</td><td>Physique</td></tr>
</table>

La structure d'informations de gestion de SNMP est conforme à celle de SMI. Ainsi, pour nommer les objets au sein d'une MIB, SNMP procède de deux façons :

- la première est un nom unique par objet (ex: sysUpTime),
- la seconde utilise les notations d'ASN.1 (Abstract Syntax Notation).

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Et vue que la classification des objets est arborescente dans le MIT, on identifie un objet en parcourant dans l'arborescence le plus court chemin qui conduit jusqu'à à ce dernier, en partant de la racine du MIT, conformément au codage ASN.1.
SNMP est un protocole qui fonctionne de manière asynchrone en ce qui concerne les requêtes/réponses. Ceci a pour but de faire en sorte qu'une entité SNMP ne soit pas pénalisé par les délais que peuvent occasionner ses demandes après formulation d'une requête ou d'une réponse à une requête. Parmi les événements importants que peuvent envoyer les agents SNMP, il y a les alarmes (ou trap, en anglais). Mais la réception de ce type de message aboutit au NMS par un canal différent. Voyons pourquoi.
De part sa position dans le modèle OSI, nous pouvons constater que le SNMP est un service qui fonctionne au-dessus de la couche de transport UDP. De ce fait, il a besoin qu'un port lui soit affecté pour qu'il puisse communiquer. En fait, on constate que 2 ports lui sont réservés : 161 et 162. Habituellement, la station d'administration formule ses requêtes en passant par le port 161 en direction de l'agent qui les reçoit aussi par le port 161. Cet agent renvoie ses réponses par le même port 161 à la station d'administration qui reçoit cette information toujours par le port 161. Mais lorsqu'il s'agit d'une alarme, l'agent l'émet toujours par le port 161, mais de part la nature du message, ce dernier est reçu par la station d'administration par le port 162. L'alarme (trap) est considéré comme un évènement « extraordinaire » (***trap***).
Pour récapituler, voici les différents cas de figure dans lesquels on peut se trouver, en ce qui concerne les requêtes et les réponses.

Il existe quatre sortes de requêtes :

- GetRequest : obtenir une variable.
- GetNextRequest : obtenir variable suivante (si existante, sinon retour d'erreur).
- GetBulk : permet la recherche d'un ensemble de variables regroupées.
- SetRequest : modifier la valeur d'une variable.

Puis, les réponses :

- GetResponse : permet à l'agent de retourner la réponse au NMS.
- NoSuchObject : informe le NMS que la variable n'est pas dispionible.

Les types d'erreurs sont les suivants : NoAccess, WrongLenght, WrongValue, WeongType, NoCreatio, WrongEncoding, NoWritable et AuthorisationError.

Les alertes (traps) sont ColdStart, WarmStart, LinkUP et AuthentificationFailure.
Il existe 3 versions du protocole SNMP : SNMPv1, SNMPv2 et SNMPv3.

La version 1, ***SNMPv1***, demeure encore la plus largement utilisée. Elle utilise la MIB I. Son grand défaut est qu'il utilise de manière non cryptée le nom de communauté pour accéder à un agent. Le pirates raffolent par conséquent cette version tout à fait docile du SNMP. CE qui n'est pas du goût d'un bon nombre d'administrateurs de réseaux !

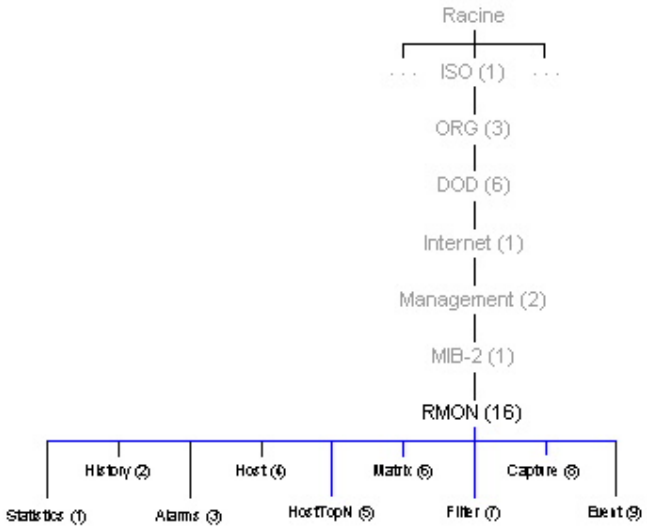
La version 2, ***SNMPv2***, est beaucoup plus complexe que la version 1. Elle contient un niveau hiérarchique d'administration plus élevé, ce qui permet d'avoir dans le réseau un administrateur central et des administrateurs secondaires. Elle incorpore aussi un niveau plus élevé en ce qui concerne la sécurité, contient une gamme de message d'erreurs plus vaste, utilise les MIB I et MIB II. Son champs d'action se trouve ainsi amélioré. La version 2 n'a cependant pas encore réussi à remplacer la version 1 du protocole. Ce qui est normal car il ne s' s'agît pas encore de la version « définitive » (*Full Standard*), mais d'une ébauche (*Draft Standard*), la version 1 donnant encore de très bons résultats.

La version 3, ***SNMPv3***, pour sa part n'est pas encore au point. Mais il a été prévu qu'elle vienne en remplacement de SNMPv1… *pour peu que tout le monde se mette d'accord sur ce point*. Le débat est encore ouvert !). Cette version comprend « un module de sécurité plus élevée, un module de traitements de messages, des modules d'application et du répartiteur de paquets ». SNMPv3 est compatible et peut cohabiter avec les versions précédentes.

Le RMON

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

La MIB RMON (Remote MONitoring) est une « extension » de la MIB II. Son identificateur au sein du sous-arbre est le numéro 16, ce qui lui donne pour OID (*Objet IDentifier*) le **1.3.6.1.2.1.16**. La MIB RMON contient 9 branches pour la assurer l'administration de tout un ensemble de supports réseaux dont Ethernet, FDDI et Token-Ring. Les 2 versions de la MIB sont chacune dotée d'un RMON qui se différencient par leurs appellation. Ainsi RMON est la version standard tandis que RMON 2 va avec la MIB II.



Arborescence de la MIB RMON

- Groupe Statistics - Contient toutes les informations associées au fonctionnement d'un réseau local ethernet. (performances temps réel, Nbr d'octets sur le réseau, Nbr de paquets, Répartition par taille de paquets, Multicoats, Broadcasts, CRC/Align, Jabbers, Fragments (Runts), OversizePackets, UndersizePackets, Collisions)

- **Groupe History** - Définition de campagnes de collectes permettant d'avoir des informations sur des indicateurs réseau. (performances temps différé, Nbr d'octets, Nbr de paquets, Broadcasts, Multicasts, CRC/AllignErrors, Undersize Paquets, Oversize Paquets, Fragments (Runts), Jabbers, Collisions, Estimation de l'utilisation en % du réseau pendant la collecte)

- **Groupe Alarm -** Paramétrage des alarmes, Objet concerné, Variation ou valeur absolue, Intervalle de mesure, mode de déclenchement (seuil en montée, descente), Valeur du seuil en montée, Valeur du seuil en descente, Pointeur vers la table d'actions (Groupe EVENT))

- **Groupe Host -** Contient les informations de trafics associées à chaque nœud Ethernet découvert (paquets émis, paquets reçus, octets émis, octets reçus, paquets erreurs émis, paquets broadcoats émis, paquets Multicasts émis)

- **Groupe HostTopN -** Définition d'études permettant d'avoir une liste d'équipements classée suivant un indicateur de trafic (Paquets reçus, Paquets émis, Octets reçus, Octets émis, Paquets erreur émis, Broadcasts émis, Multlcasts émis, Nombre d'équipements désirés, durée de la mesure)

- **Groupe Matrix -** Contient les informations de trafic entre deux équipements Ethernet (Flux échangé en octets, Flux échangé en paquets, Flux d'erreurs)

- **Groupe Filter** - Définition des filtres sur les captures de paquets (Position du filtre dans le paquet, Valeur du filtre, Masque associé au filtre, Masque complémentaire, Masque associé à l'état du paquet, Masque complémentaire, Mode de capture (paquets correspondant au filtre ou

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

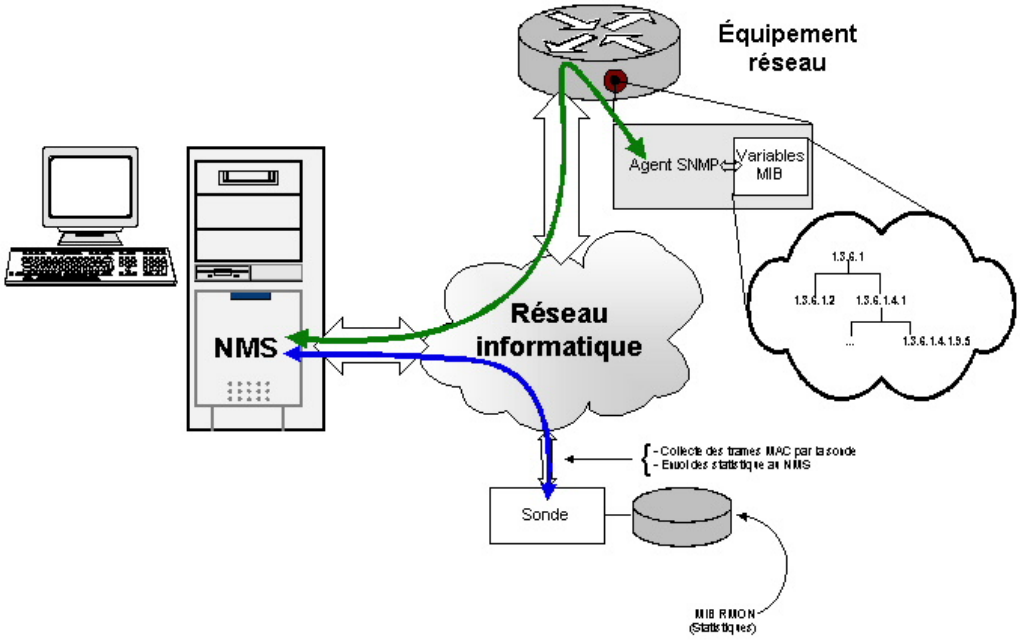
paquets complémentaires), Evénement déclenchant l'ouverture du canal, Evènement déclenchant la fermeture du canal, Nombre de paquets capturés, Evènement généré quand un paquet est capturé)

- **Groupe Packet Capture -** Gestion de l'enregistrement des paquets capturés par le Groupe Filter (No de canal utilisé, Etat de la mémoire (Buffer disponible ou saturé), Action quand le Buffer est plein, nombre d'octets enregistrés pour chaque paquet, nombre d'octets remontés par SNMPGET, Offset sur les paquets remontés, Taille désirée pour le Buffer, Nbr de Paquets capturés)

- **Groupe Event -** Définition des actions associées aux alarmes générées (communauté des Traps SNMP, Aucune action, Emission d'une alarme SNMP, Enregistrement dans la table des historiques, Table des historiques + Emission d'une alarme)

La particularité au niveau de ces différents groupes est qu'ils ne possèdent pas tous obligatoirement un agent RMON, un principe de dépendance a de ce fait été défini. Ainsi, le groupe « Alarm » a besoin de celui des évènements tandis que les groupes « HostTopN group » et « Capture group » s'appuient sur la présence du groupe « Hosts »

L'administration réseau bénéficie de l'implantation locale de sondes pour réaliser des mesures pratiquement impossibles à distance en environnement architecturé autour de routeurs ou de commutateurs. Ce procédé réduit ainsi la charge de trafic occasionnée par les fréquents échanges nécessaires à l'administration réseau pour la constitution de statistiques réalisées par un matériel ne supportant que SNMP. remplacés par les échanges de statistiques préétablies entre la station et la sonde.



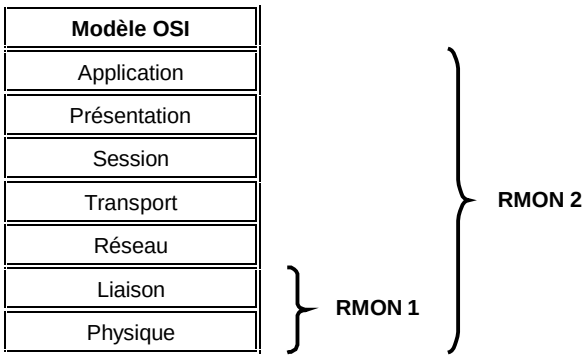
Sonde RMON sur un réseau

RMON a été mis au point par l'IETF (*Internet Engineering Task Force*) afin d'étendre les possibilités de SNMP. Les sondes connectées sur différents segments du réseau en fournissent des mesures détaillées de l'activité, au niveau 2 (pour la première version) au niveau 3 du modèle OSI (pour RMON 2), en utilisant des variables MIB et les protocoles SNMP. Ainsi, là où le processus centralisé recueillerait des informations d'administration, ces sondes rapatrient des informations vers la plate - forme d'administration pour un traitement graphique et les enregistrent éventuellement dans une base des données afin de constituer un historique de l'état du réseau. Les sondes peuvent ainsi prendre l'initiative de collecter presque toutes les trames MAC qui transitent par le réseau, tel que spécifié

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

dans les variables MIB. La MIB peut aussi être paramétrée de telle manière qu'à certains seuils les sondes déclenchent des alarmes à l'aide de traps SNMP.

Malgré l'utilité et l'intérêt évidents de RMON, il y a des limitat ions à cette technologie. Celles-ci sont intrinsèques à RMON car il s'adresse que les deux premières couches du modèle ISO (Physique et liaison). Par conséquent, une sonde RMON ne pourra analyser que le segment sur lequel elle se trouve, et cette analyse se fera au niveau MAC (couche 2 liaison). La reconnaissance des protocoles et de son adressage ne pourront se faire dans RMON que si on lui adjoint des groupes de MIB qui s'adressent aux couches supérieures du modèle ISO.



***Champs d'action de RMON 1 et RMON 2 par rapport au modèle OSI*.**

Les performances de RMON - rebaptiser RMON 1, pour les circonstances - devront donc être rehausser par de nouvelles spécifications de manière à lui permettre de remonter jusqu'à la couche de niveau 7 (Application) du modèle OSI. Ce nouveau procédé permettra au RMON de traiter les informations extraites et de les faire remonter sur la console de surveillance. La MIB RMON 2, s'appuyant sur les spécification de la MIB RMON 1, devrait ainsi posséder les caractéristiques ci - dessous :

- **Protocol Directory** définit les protocoles que la sonde peut analyser.
- **Protocol Distribution** prend les statistiques suivant le protocole.
- **Address Mapping** fait la relation entre l'adresse MAC et l'adresse du protocole (ex: MAC -> IP).
- **Network layer Host** mesure globale des trames suivant le protocole (plus cantonné au segment).
- **Network layer Matrix** mesure entre deux hosts (pas forcément dans le même segment).
- **Application layer Host** nous montons vers les couches hautes de l'OSI pour faire not re analyse.
- **Application layer Matrix** mesure entre deux hosts (suivant le protocole applicatif).
- **History** mémorise les statistiques de niveau 3 en local.
- **Probe configuration** normalisation de la configuration d'une sonde à partir du manager.

Ainsi, grâce à l'analyse approfondie des trames, l'administrateur pourra avoir une « vision » complète du réseau géré. L'administrateur réseau pourra ainsi déterminer avec précision une station de travail dont le fonctionnement perturbe le réseau. La MIB RMON 1 ne p ermettait pas simplement cette fonction car les informations (adresses physiques des stations) contenues dans les couches superficielles de la trame étaient bloquées par les routeurs.

Le document final du groupe de travail « RMON 2 » de l'IETF était soumis à la standardisation en décembre 1995.

Analyseurs de réseau

Il est plus que nécessaire de savoir qu'existe aussi sur le marché d'autres sortes d'outils qui permettent une administration de réseau de manière très optimale. Ces outils sont des appareils é lectroniques appelés analyseurs de réseau, sauf que ceux-là uniquement dédiés « analyses de réseau ». Ces appareils ne savent rien faire d'autres, mais ce qu'ils font, ils le réalisent de manière très optimale. De nombreux constructeurs en proposent. Vous avez ainsi des certificateurs de câblage réseaux, des

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

analyseurs de spectres, des sniffers, des scanners, etc… Des constructeurs tels que FLUKE, 3Com, IBM, Hewlett-Packard, Cisco, (et il y en a bien d'autres) vous en proposent toute une panoplie de ces outils dont un administrateur de réseau ne saurait se passer que très difficilement.

Alors, concernant leur mode de fonctionnement, on connecte les analyseurs de réseaux comme un poste de travail, c'est-à-dire directement sur le réseau à administrer. Ce qui leur donne la possibilité d'observer et de récupérer tout ce qui se passe sur le nœud où il sont branchés. Etant donné que Les réseaux locaux fonctionnent par diffusion, les analyseurs réseaux pourront observer, récupérer et afficher sur leurs écrans tout le trafic du sous-réseau. Les analyseurs de réseaux ont aussi la possibilité d'afficher sur leurs écran plusieurs autres types d'information dont :

- l'affichage des trames collectées,
- le filtrage des trames,
- l'instant exact du passage d'une trame,
- compter des paquets et leurs tailles moyennes,
- déterminer le nombre de collision,
- …

Avec les analyseurs de réseaux, il nous est aussi donner la possibilité de les paramétrer afin que ces derniers puissent se déclencher soit, à partir d'une heure donnée, soit su ite à certains évènements, soit une combinaison de tout çà. Il est aisé de se rendre compte qu'avec de tels outils, l'administration de réseaux peut être extrêmement simplifier. De plus, l'analyseur peut déclencher l'analyse par rapport à une heure mais aussi par rapport à un évènement ou une suite d'événements. L'un des inconvénients des analyseurs de réseaux est qu'ils se limitent au sous-réseau qu'ils observent ! Mais on finit par s'y faire.

Parmi l'innombrable produits qui existent sur le marché des analyseurs de réseaux, nous pouvons citer quelques uns.

- **L'Optiview de FLUKE™**

- Visualisation complète du réseau en quelques secondes
- Combine l'analyse de protocoles sur les sept couches OSI, la détection active, l'analyse des périphériques SNMP, l'analyse du trafic RMON2 et le test des couches physiques en une seule solution mobile
- La conception et l'interface utilisateur offrent un même niveau d'efficacité, que l'unité soit portable ou placée en liaison réseau semi-permanente
- L'analyse distante via le Web permet à sept utilisateurs d'accéder en même temps à une seule unité

- **CiscoWorks2000 Campus Manager de Cisco™**

Campus Manager dispose grâce à Topology Services, User Tracking, Path Analysis et l'affectation de port VLAN/LANE d'une large gamme de fonctions qui permettent aux administrateurs réseau de mieux comprendre, surveiller, configurer, diagnostiquer leur réseau ou de réagir aux changements d'infrastructure.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Campus Manager 3,1 permet d'afficher des cartes de topologie réseau de différentes façons, d'une représentation à plat de la couche 2 jusqu'à des vues abstraites plus représentatives ou plus extensibles vers des réseaux de site de grande dimension. Ces abstractions se répartissent en deux groupes : domaines gérés et vues réseau. Les domaines gérés sont des vues topologiques des groupes logiques de périphériques organisés en tissu commuté ATM et en domaines VTP. Les vues réseau sont des représentations physiques du réseau et organisées en vues complètes ou abstraites, par exemple vues des limites du réseau local, vues de couche 2, vues des périphériques non connectés ou vues VTP.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

VIII-ANALYSE DES BESOINS EN CE QUI A TRAIT A L'INSTALLATION D'UN SERVEUR RESEAU

VIII-1- LA DEMARCHE DE CONCEPTION D'UN RESEAU

Lorsque l'on arrive à ce stade, et au vu de tout ce que nous avons déjà étudié, il faut alors s'armer de beaucoup de prudence et de bon sens. Il ne faut pas oublier que la technologie évolue à grande vitesse et de ce fait, vous serez constamment amener à remettre question votre étude. C'est un grand défi que de vouloir concevoir un réseau lorsque le trafic qu'il doit générer est important. Il ne suffit pas en effet de posséder tous les équipements entrant en jeu dans cette phase de conception (micro -ordinateurs, câbles, connecteurs, interfaces, imprimantes, systèmes d'exploitation, etc…), il faut savoir maîtriser sa mise en œuvre de manière à ce que le réseau puisse être évolutif et facilement administrable. Mais fort heureusement, ce défi n'est pas insurmontable malgré les difficultés que peut poser la conception d'un réseau contenant des milliers de nœuds.

Il n'y a pas de doute que vous autres administrateurs et architectes de réseaux êtes conscients que tous les composants de votre réseau possèdent des exigences particulières. Vous pouvez constater que la conception d'un réseau peut constituer un défi de taille vu que cette tâche dépasse largement le simple branchement d'ordinateurs entre eux. Vous n'êtes pas non plus sans savoir que votre réseau, une fois défini, vous devez en documenter largement les objectifs. Ces objectifs sont en général les suivants :

- **Fonctionnalité** – Le réseau doit répondre aux exigences des utilisateurs pour leur travail. Le réseau doit offrir la connectivité utilisateur-utilisateur et utilisateur-application avec une vitesse et une fiabilité adéquates.
- **Evolutivité** - La conception initiale du réseau doit pouvoir croître sans qu'il ne soit nécessaire d'apporter des modifications importantes à la conception globale.
- **Adaptabilité** - Le réseau doit être conçu en fonction des technologies futures et ne doit pas comporter d'éléments susceptibles d'entraver la mise en œuvre de nouvelles technologies, à mesure qu'elles deviennent disponibles.
- **Facilité de gestion** - La conception d'un réseau doit en favoriser la surveillance et la gestion afin d'assurer la stabilité de gestion de ce réseau.

Venons-en au fait concrètement et essayons de voir ensemble comment bâtir un réseau de manière pratique.

Pour bien concevoir un réseau, vous aurez besoin en tête une bonne stratégie d'approche. Vous économiserez ainsi bien de déboires et vous n'aurez pas besoin de vous lancer tête baissée d ans le câblage. Ainsi, nous allons vous guider à travers les mailles de différentes architectures (logiques et physiques) afin de vous aider à mieux cerner la manière de procéder lorsque vous serez confrontés à diverses situations.

Première étape :
Avant d'aller plus en avant, il va falloir trouver des réponses à des questions du genre :
Pour quelles fins servira le réseau ?
Y-aura-t-il besoin de partager de simples documents, et/ou de documents très volumineux tels que les fichiers graphiques de CAO ?
Aura-t-on besoin de d'un réseau capable de supporter la charge de la visioconférence ?
Le serveur de fichiers stockera-t-il des données partagées ?

Il Faudra prendre le temps nécessaire pour penser à toutes les éventualités possibles que vous jugerez nécessaires.

Deuxième étape :
Il faudra essayer de déterminer la durée de vie et le degré d'évolutivité du réseau que l'on veut mettre en place, car il ne faudra pas perdre de vue que la technologie évolue à grande vitesse. Vous n'aimeriez pas que votre réseau devienne obsolète de deux ans seulement après sa mise en service !

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Troisième étape :
Voudrez-vous que chaque utilisateurs aient leurs logiciels de travail directement installés dans leurs postes de travail (*thick clients* ou gros clients) ou que chacun aille charger son application directement à partir du serveur (*thin clients* ou petits clients) ? Dans les deux cas on pourra mettre en valeur les avantages et les inconvénients :

En ce qui concerne les « gros clients », tous les logiciels d'application sont installés sur leurs postes de travail :
Avantages : l'indisponibilité du réseau ne pénalisera pas les utilisateurs qui pourront poursuivre leurs travaux en local. Seules les ressources partagées ne seront pas disponibles.
Inconvénients : Pour les mises à jours des applications, il faudra se lever de bonheur et prendre son mal en patience, surtout qu'il y a beaucoup d'utilisateurs qui ne sont pas très familiarisés avec l'outil informatique. Il ne sera donc pas question de compter sur eux pour vous apporter une bouffée d'oxygène en vous aidant dans cette tâche.

En ce qui concerne les « petits clients », tous les logiciels sont installés sur un serveur d'applications :
Avantages : La mise à jour des applications s'avère être beaucoup plus simple. Il n'y aura qu'à la réaliser uniquement sur le serveur, et tout le monde la possède en même temps
Inconvénients : Lorsque le réseau tombe… vous tombez avec lui !

Personnellement, je trouve la solution des « gros clients » plus intéressante. Les logiciels ne sont pas très souvent mis à jours dans de grandes structures. Si vous optez pour la solution d'un réseau de « petits clients », il faudra alors que vous réfléchissiez très sérieusement à l'option de doter les serveurs de la technologie RAID 5 pour les mémoires de masse et d'alimentations électriques redondantes. Eh oui, vous aurez besoin de plus d'un serveur de fichiers !

Quatrième étape :
Il faut commencer à réfléchir sur l'architecture globale du réseau. Il faudra surtout vous axer sur deux aspects : l'architecture physique et l'architecture logique du réseau.

L'architecture physique concernera le câblage, les commutateurs, les routeurs, etc… Il faudra retenir l'emplacement géographique des serveurs afin de faire en sorte que l'administration soit relativement simplifiée. C'est aussi à ce niveau que vous déterminerez les équipements de la couche physique du réseau. Voici un certain nombre d'architectures physiques.

- **L'architecture en bus**. Comme vous le savez, c'est un réseau linéaire avec les serveurs connectés sur l'un des bouts et tous les clients connectés à différents points du réseau, que l'on peut considérer comme étant fédérateur. Le réseau en bus ne donne pas beaucoup de marge de manœuvre et de flexibilité. C'est cependant excellent pour un petit réseau local où l'option d'évolutivité ne sera pas tellement prise en compte. Le grand inconvénient de cette architecture est que lorsqu'une section tombe en panne, une bonne partie du réseau pourra en être affectée.
- En ce qui concerne **l'architecture en étoile**, elle utilise à volonté des commutateurs ou des concentrateurs architecturés autour d'un commutateur ou d'un concentrateur central auquel tous les serveurs seront connectés. Une telle architecture est très flexible. Si vous avez besoin de plus de connexions, vous n'avez qu'à rajouter d'autres commutateurs ou concentrateurs proche de l'endroit à desservir. Il faudra simplement s'assurer d'avoir en réserve quelques concentrateurs ou commutateurs supplémentaires pour le cas où le point de connexion des serveurs arrivaient à vous faire un faut bon.
- Vous pourrez aussi imaginer une architecture **hétérogène** (une combinaison des deux architectures citées plus haut). Une architecture en bus pour relier tous les serveurs et une architectures en étoile pour tous les autres postes de travail clients. Ce modèle d'architecture est très apprécié dans les grands réseaux ou lorsqu'il n'est pas possible de garder tous les serveurs au même endroit

Pour le cas de **l'architecture logique**, il s'agit de savoir si vous aurez besoin de plus d'une adresse IP pour votre réseau. Si vous devez gérer un réseau avec moins de deux cents postes de travail, un réseau

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

de la classe « C » fera largement l'affaire. Vous pourrez gérer suffisamment d'adresses IP pour vos actuels différents nœuds, avec la possibilité d'augmenter quelques équipements dans l'avenir. Il ne faudra pas confondre la topologie logique de votre réseau avec les différents départements de votre institution : chaque département n'aura pas besoin de son propre sous-réseau. Et si des fois, vos amis de la Comptabilité décident qu'ils n'auront pas besoin d'avoir accès aux données et aux serveurs du département de CAO, vous aurez toujours la possibilité de les relocaliser sur un réseau physique et logique différent, voire dans un autre VLAN ! De plus, vous aurez la possibilité de réduire considérablement les domaines de diffusion et d'accroître le débit du réseau.

On ne saura que mieux vous conseiller de faire en sorte que votre réseau soit le plus simple possible. S'il vous est possible de concevoir un réseau architecturé autour d'une seule adresse IP, alors réalisez-le ainsi ! Gardez toujours à l'esprit que deux réseaux ayant des adresses IP différentes ne pourront pas communiquer directement ensemble. Il faudra munir chacun d'un routeur s'il y a besoin de partager des ressources. Si vous ne prenez pas les bonnes précautions, vous risquez de concevoir un réseau qui exigera de vous plus de 60 heures de votre temps chaque semaine !

Cinquième étape :
Prenez le temps nécessaire pour passer en revue le réseau tel que vous aimeriez qu'il soit conçu et en comparant le tout avec les attentes des futurs utilisateurs. Il faudra que tous les utilisateurs soient sensibilisés à l'idées que vu que vous arrivez au stade de la réalisation pratique, ce sont là les toutes dernières concessions que vous ferez pour la conception du réseau. Une fois que vous aurez commencé de passer les câbles et de concevoir vos différentes connexions, il ne vous sera plus possible de procéder à de grandes modifications… sauf cas de force majeurs bien entendu (car je vous vois mal en train de refuser de céder aux exigences de dernière minute de votre employeur, par exemple !).

Encore autre chose : dans le passé, les administrateurs de réseaux devaient choisir entre les réseaux Ethernet partagés et les réseaux commutés en se basant sur le rapport qualité/prix. Mais au vu de la baisse considérable du prix des commutateurs, il n'est plus raisonnable de nos jours de concevoir des réseaux sur cette base. Mais rappelons un peu la différence entre ces deux types de réseaux.

Dans les réseaux Ethernet partagés, toute la bande passante est partagée par chaque nœud. Lorsqu'un nœud est en transmission, tous les autres devaient attendre la fin de cette transmission avant de rentrer en compétition pour savoir lequel des autres nœuds allaient réussir à reprendre le relais pour transmettre à son tour. S'il arrive que deux nœuds transmettent en même temps, il y a alors la fatale collision et les données devront être retransmises. Pour de petit réseaux, ou encore lorsque vous n'avez pas à gérer de gros volumes de données, alors ce type de réseau fera largement votre affaire. Et vu qu'un nœud récupère tout juste des données et les envoie à tous les autres périphériques connectés, vous pourrez vous contenter d'utiliser un concentrateur dans un réseau local Ethernet avec du câble UTP.

Par contre, un commutateur est doté d'une mémoire tampon qui lui permet de stocker temporairement les paquets qui doivent êtres acheminés vers les autres nœuds. Chaque poste de travail possède sa propre bande passante dédiée et n'aura jamais à attendre qu'un nœud soit libéré pour commencer à transmettre. Les collisions sont ainsi minimisées et peuvent être presque inexistantes. Les commutateurs sont conçus pour « connaître » automatiquement les adresses MAC (Medium Access Control) des équipements qui leurs seront connectés. Ainsi, rajouter de nouveaux postes de travail devient beaucoup plus simple : il n'y a qu'à le brancher et le commutateur « voit » la nouvelle connexion et commence à lui faire parvenir des données. On ne saurait que mieux vous conseiller pour l'option du réseau Ethernet commuté vu que les prix sont très abordables de nos jours. Certains commutateurs ont même la capacité de « dialoguer » entre eux pour voir comment accroître la bande passante. Et enfin, vous aurez assez de bon sens pour interconnecter vos commutateurs en passant par différents chemins, ce qui aura pour avantage de faire en sorte que même si un des câbles arrivait à être coupé accidentellement, la liaison reste maintenue entre les commutateurs. Vous aurez ainsi créer des ligne de réserves intercommutateurs. Ce qui nous amène à la dernière étape.

Sixième étape :

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

En cas de panne de réseau, de quoi pourrez-vous bien avoir besoin pour le dépannage ? Pensez à garder des câbles de rechange, des connecteurs, des cartes réseau (NIC), voire même des commutateurs supplémentaires et une bonne dose d'idées originales ! Evitez de connecter directement vos équipements aux commutateurs. Passer par des panneau x de brassage qui serviront de relais entre les commutateurs et les différents périphériques du réseaux, ce sera plus simple pour isoler les pannes. Surtout, utilisez des câbles catégorie 5/5e (au moins). Il faudra enfin pouvoir disposer d'analyseurs de réseaux. Muni de tout çà, vous êtes fins prêts pour concevoir votre réseau.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

IX- OUTILS DE VERIFICATION DE L'INSTALLATION COMMANDES TCP/IP

IX-1- PING

Vérifie les connexions avec un ou plusieurs ordinateurs distants. Cette commande est disponible uniquement si le protocole TCP/IP est installé.

ping [**-t**] [**-a**] [**-n** *compte*] [**-l** *longueur*] [**-f**] [**-i** *ttl*] [**-v** *tos*] [**-r** *compte*] [**-s** *compte*] [[**-j** *liste-ordinateurs*] | [**-k** *liste-ordinateurs*]] [**-w** *temporisation*] *liste-destinations*

Paramètres

-t
Sollicite une réponse de l'ordinateur spécifié jusqu'à ce qu'il soit interrompu.

-a
Remplace les adresses par des noms d'ordinateur.

-n *compte*
Envoie le nombre de paquets ECHO spécifié par *compte*. La valeur par défaut est 4.

-l *longueur*
Envoie les paquets ECHO contenant le volume de données spécifié par *longueur*. La valeur par défaut est 32 octets et la valeur maximale, 65 527.

-f
Envoie un drapeau de non-fragmentation dans le paquet. Le paquet ne sera ainsi pas fragmenté par les passerelles.

-i *ttl*
Assigne au champ Durée de vie la valeur spécifiée par *ttl*.

-v *tos*
Assigne au champ Type de service la valeur spécifiée par *tos*.

-r *compte*
Enregistre l'itinéraire du paquet sortant et du paquet en retour dans le champ Route enregistrée. Le paramètre *compte* permet de spécifier 1 ordinateur minimum et 9 ordinateurs maximum.

-s *compte*
Spécifie le marquage de temps pour le nombre de tronçons spécifié par *compte*.

-j *liste_ordinateurs*
Achemine des paquets selon la liste des ordinateurs spécifiés par *liste-ordinateurs*. Les ordinateurs consécutifs peuvent être séparés par des passerelles intermédiaires (itinéraire source libre). Le nombre maximal autorisé par IP est 9.

-k *liste-ordinateurs*
Achemine des paquets selon la liste des ordinateurs spécifiés par *liste-ordinateurs*. Les ordinateurs consécutifs peuvent être séparés par des passerelles intermédiaires (itinéraire source libre). Le nombre maximal autorisé par IP est 9.

-w *temporisation*
Spécifie un intervalle de temporisation en millisecondes.

liste_destinations
Spécifie les ordinateurs distants à solliciter.

IX-2- IPCONFIG

Cette commande de diagnostic affiche toutes les valeurs de la configuration réseau TCP/IP en cours. Elle sert particulièrement sur les systèmes exécutant DHCP, car elle permet aux utilisateurs de déterminer les valeurs de la configuration TCP/IP configurées par DHCP.

ipconfig [/**all** | /**renew** [*carte*] | /**release** [*carte*]]

Paramètres

all
Affiche toutes les informations. Sans ce commutateur, **ipconfig** affiche uniquement l'adresse IP, le masque de sous-réseau et les valeurs passerelle par défaut de chaque carte réseau.

/renew [*carte*]

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Renouvelle les paramètres de configuration DHCP. Cette option est disponible uniquement sur les systèmes dotés du Service clients DHCP. Pour spécifier un nom de carte, tapez celui qui apparaît quand vous utilisez **ipconfig** sans paramètre.
/release [*carte*]
Libère la configuration DHCP actuelle. Cette option désactive TCP/IP sur le système local. Elle est disponible uniquement sur les clients DHCP. Pour spécifier un nom de carte, tapez celui qui apparaît quand vous utilisez **ipconfig** sans paramètre.
Lorsqu'il est spécifié sans paramètre, l'utilitaire **ipconfig** présente toutes les valeurs de la configuration TCP/IP en cours, y compris l'adresse IP et le masque de sous-réseau. Cet utilitaire sert particulièrement sur les systèmes exécutant DHCP, car il permet aux utilisateurs de déterminer les valeurs configurées par DHCP.

IX-3- NBTSTAT

Cette commande de diagnostic affiche les statistiques de protocole et les connexions TCP/IP en cours utilisant NBT (NetBIOS sur TCP/IP). Cette commande est disponible uniquement si le protocole TCP/IP est installé.
nbtstat [**-a** *nom_distant*] [**-A** *adresse IP*] [**-c**] [**-n**] [**-R**] [**-r**] [**-S**] [**-s**] [*intervalle*]
Paramètres
-a *nom_distant*
Affiche la table des noms de l'ordinateur distant en utilisant le nom.
-A *adresse IP*
Affiche la table des noms de l'ordinateur distant en utilisant son adresse IP.
-c
Affiche le contenu du cache de noms NetBIOS en donnant l'adresse IP de chaque nom.
-n
Affiche les noms NetBIOS locaux. La mention Registered indique que le nom est enregistré par diffusion (Bnode) ou par WINS (autres types de noeuds).
-R
Recharge le fichier Lmhosts après avoir purgé tous les noms du cache de noms NetBIOS.
-r
Affiche les statistiques de résolution de noms pour la résolution de noms en réseau Windows. Sur un système Windows 2000 configuré pour utiliser WINS, cette option renvoie le nombre de noms résolus et enregistrés par diffusion ou par WINS.
-S
Affiche les sessions client et serveur, en répertoriant les ordinateurs distants par adresse IP uniquement.
-s
Affiche les sessions client et serveur. Ce commutateur tente de convertir l'adresse IP de l'ordinateur distant en un nom à l'aide du fichier Hosts.
intervalle
Affiche les statistiques sélectionnées de manière répétée avec un *intervalle* (en secondes) entre chaque occurrence. Appuyez sur CTRL+C pour interrompre l'affichage des statistiques. Si ce paramètre est omis, nbstat n'imprime qu'une seule fois les informations de la configuration.

IX-4- NET (OPTIONS DE LA LIGNE DE COMMANDE)

Beaucoup de commandes réseau de Windows 2000 commencent par le mot **net**. Ces commandes possèdent certaines propriétés en commun :

- Vous pouvez voir apparaître la liste des commandes **net** disponibles en tapant **net /?**.
- Vous pouvez obtenir une aide sur la ligne de commandes pour connaître la syntaxe d'une commande **net** en tapant **net help** *commande*. Par exemple, pour obtenir une aide sur la commande **net accounts**, tapez **net help accounts**.
- Toutes les commandes **net** acceptent les options **/yes** et **/no** (qui peuvent être abrégées sous la forme **/y** et **/n**). L'option **/y** répond automatiquement **oui** à chaque invite interactive générée par la commande tandis que l'option **/n** répond **non**. Par exemple, **net stop server** vous invite généralement à confirmer que vous voulez bien arrêter tous les services qui dépendent du

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

service Serveur, tandis que **net stop server /y** répond automatiquement **oui** à l'invite et le service Serveur s'arrête.

IX-5- NET STATISTICS

Affiche le journal des statistiques du service Station de travail ou Serveur local ou bien les services en cours d'exécution pour lesquels des statistiques sont disponibles.

net statistics [**workstation** | **server**]

Paramètres

Aucun

Tapez **net statistics** sans paramètre pour afficher la liste des services en cours d'exécution pour lesquels des statistiques sont disponibles.

workstation

Affiche les statistiques pour le service Station de travail local.

server

Affiche les statistiques pour le service Serveur local

IX-6- NETSTAT

Affiche les statistiques de protocole et les connexions réseau TCP/IP en cours. Cette commande est disponible uniquement si le protocole TCP/IP est installé.

netstat [**-a**] [**-e**] [**-n**] [**-s**] [**-p** *protocole*] [**-r**] [*intervalle*]

Paramètres

-a

Affiche toutes les connexions et les ports d'écoute. Les connexions serveur ne sont en principe pas affichées.

-e

Affiche des statistiques relatives à Ethernet. Ce paramètre peut être combiné avec l'option **-s**.

-n

Affiche les adresses et numéros de ports sous forme numérique (au lieu de tenter des recherches par nom).

-s

Affiche les statistiques des protocoles respectifs. Par défaut, les statistiques de TCP, UDP, ICMP et IP sont affichées. L'option **-p** peut être utilisée pour spécifier un sous-ensemble des protocoles par défaut.

-p *protocole*

Affiche les connexions du protocole spécifié par le paramètre *protocole* ; ce paramètre peut avoir pour valeur **tcp** ou **udp**. Quand il est utilisé avec l'option **-s** pour afficher des statistiques par protocole, *protocol* peut prendre la valeur **tcp**, **udp**, **icmp** ou **ip**.

-r

Affiche le contenu de la table de routage.

intervalle

Affiche les statistiques sélectionnées de manière répétée avec un *intervalle* (en secondes) entre chaque occurrence. Appuyez sur CTRL+C pour interrompre l'affichage des statistiques. Si ce paramètre est omis, **netstat** n'imprime qu'une seule fois les informations de configuration.

IX-7- TRACERT

Cet utilitaire de diagnostic détermine l'itinéraire emprunté vers une destination. Pour cela, il envoie vers la destination des paquets d'écho ICMP (Internet Control Message Protocol) présentant des valeurs TTL (Time To Live) variables. Chaque routeur sur l'itinéraire décrémente la valeur TTL du paquet d'au moins 1 avant de le retransmettre. La valeur TTL correspond donc effectivement à un comptage de tronçon. Lorsque la valeur TTL d'un paquet atteint 0, le routeur est supposé renvoyer un message de dépassement de temporisation ICMP au système source. **Tracert** détermine l'itinéraire en envoyant le premier paquet d'écho dont la valeur TTL est 1 et en l'augmentant de 1 à chaque transmission ultérieure jusqu'à ce que la cible réponde ou que la valeur TTL maximale soit atteinte. L'itinéraire est obtenu en analysant les messages de dépassement de temporisation ICMP renvoyés par les routeurs intermédiaires. Toutefois, certains routeurs abandonnent, sans le signaler, des paquets dont la valeur TTL a expiré et ne sont donc pas détectés par la commande **tracert**.

tracert [**-d**] [**-h** *tronçons_maximum*] [**-j** *liste_ordinateurs*] [**-w** *temporisation*] *nom_cible*

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Paramètres

-d

Spécifie de ne pas résoudre les adresses en noms d'ordinateur.

-h *tronçons_maximum*

Spécifie le nombre maximal de tronçons pour rechercher la cible.

-j *liste_ordinateurs*

Spécifie un itinéraire source libre le long de la *liste_ordinateurs*.

-w *temporisation*

Spécifie le délai d'attente en millisecondes défini par *temporisation* pour chaque réponse.

nom_cible

Nom de l'ordinateur cible.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

X- PROJET DE CABLAGE STRUCTURE

X-1- PLANIFICATION DU PROJET

Décrire les procédures de sécurité relatives à l'installation d'un réseau

Note de l'instructeur

En quoi consiste le projet? L'objectif du projet de câblage structuré est de permettre aux étudiants de mettre en pratique les compétences apprises en classe dans le cadre d'une véritable installation de ré seau. Le projet peut prendre plusieurs formes.

Vous pouvez enseigner la matière du chapitre 9 et aider simultanément tous les étudiants à acquérir les compétences nécessaires pour chacune des phases d'une installation de câbles avant de passer à l'installa tion proprement dite. C'est la méthode privilégiée. Vous pouvez également enseigner ces compétences à un certain nombre d'étudiants et demander à un représentant de chaque groupe de transmettre ces compétences aux autres membres de son équipe. Une autre mé thode consiste à enseigner les compétences au besoin, à mesure des exigences du projet. Vous seul pouvez décider de la meilleure méthode pour vos étudiants.

Une foule de projets sont possibles. Vous pouvez câbler l'arrière de la classe, la zone où sont si tués les routeurs et le châssis de la session 2. Si l'école comprend une autre salle ou prépare un autre projet de câblage, vous pouvez obtenir l'autorisation d'exécuter ce projet. Si une autre école à proximité de la vôtre a besoin d'être câblée, vous pourriez faire le travail le samedi ou après les heures de classe. Vous pourriez également participer aux activités d'une «journée réseau» si de telles activités existent dans votre secteur. La forme du projet importe peu. Ce qui importe, c'est que les étudia nts réalisent un projet, du début à la fin.

Dans toute situation réelle de câblage, la sécurité est d'une importance cruciale. Vous devez d'abord obtenir la permission de la direction de l'école et peut -être même celle de la commission scolaire ou du repr ésentant du syndicat local. Deuxièmement, vous devrez peut -être obtenir des formules d'autorisation des étudiants eux -mêmes, particulièrement si le projet se déroule ailleurs qu'à l'école.

Voici quelques conseils sur la sécurité dans le domaine électrique . Vous devriez discuter avec vos étudiants des règles de sécurité à suivre pendant l'installation. Ne jamais travailler sur une unité (tel qu'un concentrateur, un routeur, un commutateur ou un PC) lorsque le boîtier est ouvert et que l'unité est sous tensi on (cordon d'alimentation branché). Testez les prises électriques avec un voltmètre ou un multimètre adéquat. Repérez l'emplacement des conduits électriques et des câbles d'alimentation avant l'installation des câbles de réseautage. Assurez la mise à la te rre de tout le matériel réseau. Faites attention de ne jamais taillader ou couper un fil de 120 V c.a. sous tension. Il ne s'agit là que de quelques -unes des précautions à prendre.

Il faut également prendre des précautions mécaniques. Portez toujours des verres de sécurité lorsque vous utilisez des cisailles ou une perceuse. Faites attention aux mèches et aux lames. Une vieille maxime dit «mesurez deux fois, coupez une fois». Cela signifie qu'il faut mesurer attentivement avant d'utiliser un outil. Etudiez avec les étudiants la zone de coupe ou de perçage attentivement avant de procéder. Vous ne voulez pas entrer en contact avec des câbles électriques ou autres conduits à l'intérieur des murs. Tentez de travailler proprement. Evitez de soulever de la poussi ère puisque vous installerez des unités réseau sensibles. Si vous utilisez une échelle, suivez les précautions d'usage. Discutez avec vos étudiants d'autres précautions mécaniques à prendre.

Si les précautions nécessaires sont prises, le projet de câblage structuré peut être une activité amusante et enrichissante. Mais une gestion serrée de la classe et de l'équipe est nécessaire car les dangers potentiels sont nombreux vu la nature du travail.

L'installation d'un réseau peut être une expérience fascinante, mais il ne faut jamais oublier les précautions élémentaires relatives à la sécurité. La création d'un réseau comprend des tâches qui relèvent à la fois de l'électricien et de l'ouvrier en construction. Dans les deux cas, la sécurité est primordiale.

Votre professeur discutera avec vous des procédures de sécurité en classe et des précautions élémentaires à prendre lorsque vous manipulez des matériaux de réseautage, qu'ils soient électriques ou de construction. Nous vous suggérons de discuter de cette questi on en classe pour que vous compreniez bien les raisons soutenant l'emphase constante sur la sécurité.

Matériaux électriques

La liste qui suit décrit certaines des précautions à prendre lorsque vous manipulez des matériaux électriques :

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

- Ne jamais travailler sur une unité (tel qu'un concentrateur, un routeur, un commutateur ou un PC) lorsque le boîtier est ouvert et que l'unité est sous tension (cordon d'alimentation branché).
- Testez les prises électriques avec un voltmètre ou un multimètre adéquat.
- Repérez l'emplacement des conduits électriques et des câbles d'alimentation avant d'installer les câbles de réseautage.
- Assurez la mise à la terre de tout le matériel réseau.
- Faites attention de ne jamais taillader ou couper un fil de 120 V c.a. sous tension.

Matériaux mécaniques et de construction

La liste qui suit décrit certaines des précautions à prendre lorsque vous manipulez des matériaux mécaniques et de construction :

- Portez des verres de sécurité lorsque vous coupez ou percez et faites attention aux mèches et aux lames.
- Mesurez attentivement avant de couper, de percer ou de modifier de manière permanente des matériaux de construction - «Mesurez deux fois, coupez une fois.»
- Etudiez, avec l'aide de votre professeur, les matériaux à couper ou à percer et ce, avant de commencer. Vous ne voulez pas que vos outils électriques entrent en contact avec des câbles électriques ou autres conduits à l'intérieur des murs.
- Tentez de travailler proprement (par exemple, évitez de soulever de la poussière qui peut perturber le fonctionnement d'unités réseau sensibles).
- Si vous utilisez une échelle, suivez les précautions d'usage.

Il ne s'agit là que de certaines des précautions à prendre lorsque vous manipulez des matériaux de construction de réseau. Discutez avec votre professeur et vos condisciples pour identifier d'autres mesures que vous pourriez prendre afin d'assurer votre sécurité et celle des gens qui travailleront avec vous.

Décrire la documentation du réseau - documents de planification et de l'ouvrage fini

Note de l'instructeur

Un vieil adage dit que vous recevrez de vos étudiants ce que vous attendez d'eux. Cela semble être vrai dans le cas de la documentation réseau. Nombre d'étudiants et de techniciens en réseautage n'aiment pas rédiger, mais la documentation fait partie intégrante de toute installation professionnelle de câblage. Les principales rubriques proposées sont les suivantes :

- journal technique
- topologie logique
- topologie physique
- feuille d'identification des câbles
- matrices de résolution de problèmes
- prises étiquetées
- parcours de câbles étiquetés
- sommaire des prises et des parcours de câbles
- sommaire des unités, des adresses MAC et des adresses IP

Votre projet de câblage structuré sera exécuté à la demande d'un client qui veut faire câbler une salle (ou une école). Votre première tâche, en tant que concepteur de réseau, sera de demander à votre client de préciser, par écrit, le résultat qu'il souhaite obtenir.

Votre travail de concepteur comprendra également la rédaction de la documentation, y compris les évaluations des faits, les rapports d'étapes, les rapports finaux et les rapports d'essais.

La liste qui suit comprend une partie de la documentation que vous devrez rédiger pendant le processus de planification et de conception du réseau :

- journal technique
- topologie logique

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

- topologie physique
- feuilles d'identification des câbles
- matrices de résolution de problèmes
- prises étiquetées
- parcours de câbles étiquetés
- sommaire des prises et des parcours de câbles
- sommaire des unités, des adresses MAC et des adresses IP

Demandez à votre professeur si d'autres éléments de documentation sont pertinents à votre projet.

Décrire le fonctionnement optimal d'une équipe d'installation de réseau

Note de l'instructeur

Le projet de câblage stru cturé est un projet d'équipe idéal. Comme dans tout projet d'équipe, il existe un équilibre entre les responsabilités du groupe et celles des individus. Une façon d'atteindre cet équilibre est d'attribuer des tâches différentes à chaque membre de l'équipe et d'attribuer à chacun une note individuelle et une note de groupe à la fin du projet. Il existe plusieurs façons de créer des groupes et des rôles de groupe; voici une suggestion :

Responsable des matériaux et des outils : Cet étudiant a la charge des co ffres à outils, des câbles, des connecteurs et des dispositifs de vérification.

Responsable de l'acheminement des câbles : Cet étudiant est responsable de la planification et de l'acheminement des câbles conformément aux normes électriques et de sécurité, ainsi que de la vérification du parcours du câble.

Responsable des connexions aux prises et au tableau de connexions : Cet étudiant doit effectuer des raccordements de qualité, installer des prises et les tester.

Chef de projet (responsable de la sécurité) : Cet étudiant est chargé de gérer le travail des autres membres de l'équipe. Il doit également s'assurer que toute la documentation nécessaire est rédigée. Il assure aussi la communication avec le professeur.

Effectuez une rotation des rôles pour que tou s les étudiants puissent acquérir les compétences de chaque poste. Les professionnels du réseautage travaillent souvent en équipe et doivent assumer différentes tâches, soyez polyvalents.

Une des méthodes de travail les plus efficaces pour l'installation d'un réseau consiste à subdiviser l'équipe en petits groupes d'une personne ou plus. Nous vous recommandons de changer de rôle périodiquement avec d'autres membres de votre équipe d'installation pour que chaque étudiant ait l'occasion d'exécuter différentes tâches. Cela vous permettra de développer les compétences nécessaires à l'installation d'un réseau tout en apprenant à travailler avec d'autres au sein d'une équipe.

La liste qui suit décrit certaines des tâches qui peuvent être attribuées aux petites éq uipes :

- *Chef de projet* - Ses responsabilités comprennent :
  - Mettre en oeuvre les mesures de sécurités
  - Voir à la documentation des matériaux et des activités
  - S'assurer que les membres de l'équipe accomplissent leurs tâches
  - Communiquer avec le professeur
- *Responsable des matériaux et des outils* Cet étudiant a la charge des coffres à outils, des câbles, des connecteurs et des dispositifs de vérification
- *Responsable de l'acheminement des câbles* - Cet étudiant est responsable de la planification et de l'acheminement des câbles conformément aux normes électriques et de sécurité ainsi que de la vérification du parcours du câble
- *Responsable du raccordement aux prises et au tableau de connexions* - Cet étudiant doit effectuer des raccordements de qualité, installer des prises et les tester

Planifier le déroulement du travail

Note de l'instructeur:

Un projet important de câblage structuré comprend une séquence complexe d'événements. Sans une planification adéquate de la part du professeur et de chacun des groupes, un bon nombre d'étudiants se retrouveront à attendre que quelque chose se passe. Il s'agit, bien sûr, d'une mise en garde relative à la gestion de la classe et aux questions de sécurité.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Nous vous suggérons d'aider les étudiants à créer un échéancier du p rojet et une répartition des tâches. Après avoir étudié le chapitre 9 et analysé l'emplacement du projet de câblage, les étudiants devraient avoir une bonne idée des tâches à exécuter et de leur séquence. Cela nous amène à discuter du flux des matériaux.

Pour vous assurer que le projet soit exécuté correctement, sans omissions et dans les délais prévus, nous vous suggérons de créer un organigramme notant toutes les tâches à exécuter ainsi que la séquence à suivre. L'organigramme devrait aussi indiquer l'éch éancier de chacune des tâches.

L'organigramme devrait comprendre les tâches qui suivent :

- Installation des prises
- Installation des prises
- Acheminement des câbles
- Raccordement des câbles aux tableaux de connexions
- Vérification des câbles
- Documentation des câbles
- Installation des cartes réseau
- Installation des concentrateurs, des commutateurs, des ponts et des routeurs
- Configuration des routeurs
- Installation et configuration des PC

Planifier le déplacement des matériaux

Note d'instructeur

De quoi aurez-vous besoin pour un projet de câblage structuré? Les quantités varieront considérablement selon le projet choisi.

Voici une liste des matériaux de base :

Câble à paires torsadées non blindées Plenum de catégorie 5 (câble plein)

Fiches RJ-45 (connecteurs)

Prises RJ-45

Boîtier de montage encastré ou en saillie RJ45 et matériel connexe pour tenir les prises

Tableaux de connexions RJ-45

Attaches de câbles

Velcro

Canalisation, gouttière ou conduit

Outils :

Dispositif de vérification des câbles -- Fluke 620 ou équivalent

Coupefil ou pinces à dénuder

Pince à sertir RJ-45

Outil de raccordement RJ-45

Scie à métaux

Scie à clé

Aspirateur

Verres de sécurité

Pour construire un réseau, vous aurez besoin de divers matériaux dont des outils et des ma tériaux de construction. Vous aurez besoin de certains de ces matériaux dès le début du projet alors que d'autres ne seront nécessaires qu'en cours de projet. Planifiez vos besoins et l'acquisition des matériaux bien avant la date prévue pour le début du projet.

Votre plan devrait comprendre les éléments qui suivent :

- Matériaux de construction
- Fournisseurs
- Outils

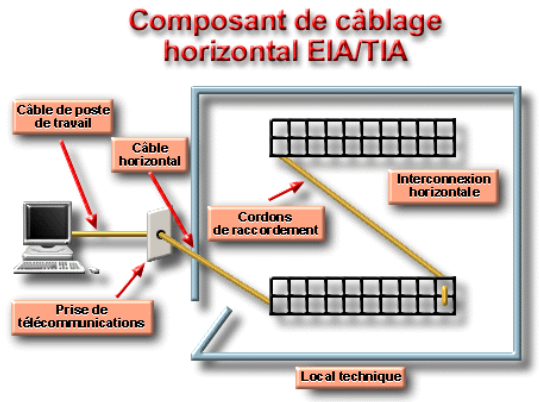
Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

- Date et durée d'utilisation des outils

X-2- INSTALLATION DES PRISES DE COURANT ET DES PRISES RJ-45

Révision des normes EIA-TIA 568-B

Note de l'instructeur:
Le schéma des normes EIA-TIA/568 est tiré d'un chapitre précédent. Faites comprendre aux étudiants que chaque «maillon de la chaîne» est géré par des normes. Dans cette section, les normes qui régissent les prises seront étudiées.



Vous savez déjà que le câblage horizontal, tel que défini par la norme EIA/TIA-568B, est le média de réseautage qui relie la sortie de télécommunications à l'interconnexion horizontale. Dans ce chapitre, vous apprendrez comment le média de réseautage est relié à la prise de télécommunications.

Décrire une prise (selon l'EIA-TIA 568-B) destinée à une prise de télécommunication

Note de l'instructeur:
Une prise EIA/TIA-568 est décrite de manière détaillée. Bien que les étudiants les connaissent peutêtre déjà, il peut être utile de faire circuler ces prises dans la classe et de revoir les configurations de broches, les voies de conductivité et les codes de couleurs avec les étudiants.

La norme EIA/TIA-568B précise que, au sein d'un système de câblage horizontal, il faut utiliser une prise RJ45 pour raccorder le câble à paires torsadées non blindées de catégorie 5 à la prise de télécommunications. La prise RJ45 contient des emplacements codés par couleur dans lesquels les fils sont insérés afin d'établir la connexion électrique. La prise contient aussi une partie femelle qui ressemble à une prise téléphonique standard sauf que la prise RJ45 comporte huit broches alors qu'une la prise téléphonique standard n'en a que quatre.

Expliquer comment monter une prise RJ-45

Note de l'instructeur:
Les deux principales méthodes de montage des prises RJ-45, le montage en saillie et le montage encastré, sont décrites. Faites circuler des exemples de matériaux, si possible, afin d'aider les étudiants à visualiser les notions enseignées.

Dans un câblage horizontal, la prise de télécommunications est habituellement installée au mur. La norme EIA/TIA-568B précise deux types de montage pour l'installation d'une prise RJ-45 au mur : le montage en surface ou le montage encastré.

Expliquer comment monter une prise RJ-45 en saillie

Note de l'instructeur:
Les boîtiers à montage par vis et à montage par adhésif sont présentés comme deux méthodes de montage en saillie des prises RJ-45.

Deux types de boîtiers peuvent servir à monter une prise RJ45 en saillie sur un mur. Le premier a un endos adhésif. Il est à noter que si vous optez pour cette méthode, vous ne pourrez pas déplacer le boîtier après son installation. Ce facteur peut être important si vous prévoyez que l'utilisation ou la configuration de la pièce risque de changer. Le deuxième type de boîtier est fixé au moyen de vis. Peu importe le type de boîtier choisi, il suffit d'insérer la prise à l'endroit approprié à l'intérieur du boîtier une fois que ce dernier est monté.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Donner certains des avantages du montage en saillie d'une prise RJ-45

Note d'instructeur:
Les avantages des prises montées en saillie par adhésif sont présentés : elles sont plus rapides à installer (ce qui réduit le coût de la main d'oeuvre) et elles sont parfois la seule option possible. Toutefois, une fois posées, il est impossible de les déplacer.

Plusieurs techniciens préfèrent les prises RJ-45 montées en saillie parce qu'elles sont plus faciles à installer. Il n'est pas nécessaire de faire de découpage dans le mur, les prises sont simplement montées à la surface du mur. Leur installation est donc plus rapide également. Cela peut devenir important lorsque le coût de la main-d'oeuvre est un facteur dans l'installation d'un réseau local. Dans certaines situations, les prises montées en saillie sont la seule solution possible.

Enumérer des facteurs à considérer avant d'encastrer une prise RJ-45

Note d'instructeur:
Cet objectif a pour but de décrire les facteurs soutenant la décision de poser une prise RJ-45 en saillie.

Il faut tenir compte de plusieurs facteurs avant d'encastrer une prise RJ45 dans un mur. Par exemple, les techniques utilisées pour couper les panneaux de gypse sont différentes de celles pour couper le plâtre. Il importe donc de déterminer, tout d'abord, le matériau qui compose le mur.

Le plâtre est souvent difficile à travailler parce qu'il s'effrite facilement. De plus, il est parfois difficile pour les vis de montage de mordre solidement dans les lattes de bois situées derrière le mur de plâtre. Dans ce cas, il peut être préférable de monter les connecteurs en saillie.

Si le mur est muni de larges plinthes en bois, songez à installer les connecteurs là car ce bois est un matériau plus solide. Si vous optez pour cette dernière solution, évitez de découper la plinthe dans les 5 cm (2 po) inférieurs de la plinthe. Si vous tentez d'installer un boîtier à cet endroit, la sablière inférieure du mur pourrait vous empêcher de l'insérer complètement. De plus, évitez d'installer des prises à des endroits vous obligeant à couper dans les moulures autour d'une porte ou d'une fenêtre.

Finalement, la dernière étape consiste à déterminer si la prise doit être montée dans un boîtier ou dans un support de montage à basse tension.

Expliquer comment encastrer une prise dans un mur de gypse

Note d'instructeur:
Nous vous suggérons de bâtir un faux mur qui servira aux trois prochains objectifs. Utilisez des 2x4 afin de créer une charpente sur laquelle vous pouvez monter des panneaux de gypse, du plâtre ou du bois pressé. Le faux mur permettra aux étudiants de pratiquer le montage encastré sans crainte d'abîmer de vrais murs. La charpente du faux mur est réutilisable, mais vous devrez remplacer périodiquement les sections de mur. Si votre école est munie d'un atelier, peut-être pourriez-vous vous adresser aux responsables. Si votre école offre des cours de métiers de la construction, proposez un projet conjoint visant à installer le câblage dans leurs projets de construction.

Si vous montez une prise dans un panneau de gypse, placez-la entre 30 et 45 cm (12 à 18 po) du plancher. Commencez par percer un petit trou à l'emplacement choisi. Déterminez ensuite si l'espace derrière l'emplacement choisi est libre. Pour ce faire, pliez un bout de fil métallique, insérez-le dans le trou et faites-le pivoter. Si le fil rencontre un obstacle, vous savez que l'espace n'est pas libre.

Dans ce cas, choisissez un nouvel emplacement à une certaine distance du trou. Percez un nouveau trou à cet endroit, insérez le fil et répétez la procédure décrite précédemment afin de déterminer si l'espace derrière le nouvel emplacement est libre.

Après avoir trouvé un emplacement approprié, vous devrez déterminer la taille de l'ouverture requise. Pour ce faire, tracez un contour au moyen du gabarit fourni avec le boîtier ou le support qui servira à encastrer la prise. Avant de couper le mur, assurez-vous que l'ouverture est droite. Utilisez un niveau.

Utilisez un canif pour découper l'ouverture. Percez le gypse avec le canif, à l'intérieur du contour dessiné, et découpez une ouverture suffisamment grande pour y insérer une scie à gypse. Insérez la scie dans le trou et sciez jusqu'à la ligne de contour. Continuez à scier le long de la ligne jusqu'à ce que vous puissiez retirer le morceau de gypse.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

L'étape suivante consiste à vérifier la taille de l'ouverture et à s'assurer que le boîtier ou le support pourra y glisser. Si vous utilisez un boîtier pour encastrer la prise, ne le fixez pas avant d'avoir acheminé le câble à l'ouverture.

Précautions
Lorsque vous travaillez à l'intérieur de murs, de plafonds ou de greniers, il est très important que vous **mettiez hors tension tous les circuits qui aboutissent à la zone de travail ou qui la traversent!** Si vous n'êtes pas certain si des fils traversent la section de l'édifice dans laquelle vous travaillez, la règle d'or est de **couper toute alimentation**.

Expliquer comment encastrer une prise dans un mur de plâtre

Note d'instructeur:
Utilisez le faux mur pour pratiquer.

Il est plus difficile de découper un mur de plâtre qu'un mur de gypse. Pour obtenir les meilleurs résultats, voici la marche à suivre. Utilisez d'abord un marteau et un ciseau pour enlever le plâtre du mur afin d'exposer la latte située dessous. Utilisez un canif pour dégager délicatement le plâtre de la latte. Placez un gabarit à plat contre la latte de sorte qu'il superpose également trois sections de la latte en haut et en bas de l'ouverture. Tracez le contour du gabarit.

Utilisez une scie électrique pour découper la portion de latte complète qui est exposée au centre de l'ouverture. Pour ce faire, faites plusieurs petites entailles, d'abord d'un côté, ensuite de l'autre. Continuez de faire ces petites entailles jusqu'à ce que vous ayez retiré la latte centrale. Faites très attention pendant cette étape. Si vous tentez de couper sur toute la longueur d'un côté avant de couper de l'autre, la scie fera vibrer la latte au moment de la seconde coupe. Cela peut faire craquer le plâtre autour de l'ouverture et le décoller de la latte. Terminez la préparation de l'ouverture en sciant des entailles dans les portions de latte inférieure et supérieure.

Expliquer comment encastrer une prise dans le bois

Note d'instructeur:
Utilisez le faux mur pour pratiquer.

Choisissez l'endroit où vous voulez placer le boîtier. Vous savez déjà que, si vous choisissez de placer une prise RJ-45 sur une plinthe en bois, vous devriez éviter de découper l'ouverture dans les 5 cm (2 po) inférieurs de la plinthe. Utilisez le boîtier comme gabarit et tracez le contour.

L'étape suivante consiste à percer un trou de départ à chaque coin du contour dessiné. Insérez une scie à guichet ou une scie sauteuse dans un des trous et sciez le long de la ligne jusqu'au trou suivant. Tournez la scie et continuez à scier jusqu'à ce que vous puissiez retirer le morceau de bois.

Expliquer comment encastrer une prise dans un mur

Note d'instructeur:
Utilisez le faux mur pour pratiquer.

Après avoir préparé l'ouverture qui recevra la prise, vous pouvez insérer celle-ci dans le mur. Si vous utilisez un boîtier pour monter la prise, tenez le câble et glissez-le dans le boîtier par une des fentes. Poussez ensuite le boîtier dans l'ouverture du mur. Utilisez les vis pour fixer le boîtier à la surface du mur. A mesure que vous vissez, le boîtier se collera de plus en plus contre le mur.

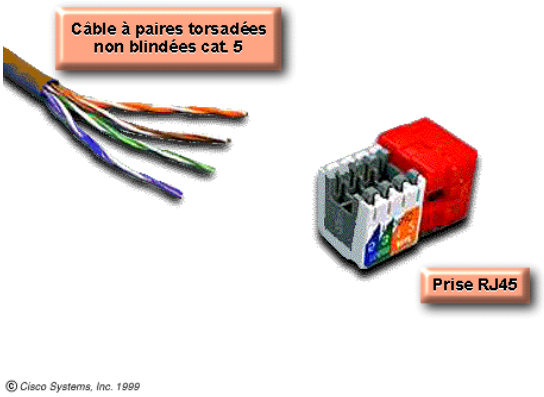
Si vous montez la prise dans un support de montage à basse tension, placez le support contre l'ouverture dans le mur. Le côté lisse devrait faire face à l'extérieur. Poussez les brides inférieure et supérieure vers l'arrière pour accrocher le support au mur. Ensuite, poussez un côté vers le haut et l'autre vers le bas pour fixer solidement le support.

Décrire la procédure pour placer les fils de cuivre du câble dans la prise

Note d'instructeur:
La meilleure façon de maîtriser cet objectif est de distribuer à chaque étudiant une prise RJ-45 et un bout de câble à paires torsadées non blindées de catégorie 5 dont la gaine a été retirée. Cela demande un peu de dextérité

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

manuelle pour placer les fils correctement dans la prise sans trop les détorsader (ce qui peut causer des problèmes de bruit).



La performance d'un réseau local est étroitement liée à la qualité de ses connexions. Lorsque des prises RJ-45 sont utilisées à la sortie de télécommunications au sein d'un système de câblage horizontal, l'ordonnancement des câbles est crucial à l'optimisation de la performance réseau. L'ordonnancement est la mise en correspondance des câbles avec les bornes appropriées.

Pour comprendre ce principe, regardez attentivement une prise RJ-45. Remarquez qu'elle porte des codes de couleur. Les couleurs (bleu, vert, orange et brun) correspondent à chacun des fils des câbles à paires torsadées non blindées de catégorie 5.

La première étape du raccordement des câbles consiste à retirer la gaine (enveloppe) de l'extrémité du câble. La longueur de gaine retirée devrait être la plus courte possible, soit environ 4 à 5 cm (1,5 à 2 po). Si la portion de câble dénudée est trop longue, le débit de transmission de données sera ralenti. Placez les fils au centre de la prise et tenez-les là pendant que vous travaillez. Des fils tordus peuvent ralentir le débit de transmission de données. De plus, assurez-vous que la portion de câble gainée sera à une distance maximale de 0,3 cm (1/8 po) de la prise.

Ensuite, triez chaque paire torsadée. La première couleur à la *gauche* de la prise est le bleu. Trouvez la paire qui contient le fil bleu et détorsadez-la. Placez le fil bleu sur la fente de *gauche* codée en bleu. Placez le second fil de cette paire sur la fente de *droite* codée en bleu et blanc.

La fente suivante du côté *droit* de la prise est verte. Trouvez la paire torsadée qui contient le fil vert et détorsadez-la. Placez le fil vert sur la fente de *droite* codée en vert. Placez le second fil de cette paire sur la fente de gauche codée en vert et blanc.

Continuez ainsi jusqu'à ce que tous les fils soient mis en correspondance avec la fente appropriée en fonction de son code de couleur dans la prise. Une fois cette étape terminée, vous êtes prêt à fixer les fils dans les fentes de la prise.

Décrire la procédure pour connecter les fils dans la prise

Note d'instructeur:

La procédure de raccordement est décrite. L'erreur la plus fréquente est que les étudiants placent la lame dans le sens inverse et coupent le fil à l'intérieur de la prise au lieu de tailler le fil superflu à l'extérieur de la prise. Il pourrait être utile de souligner que cette procédure sert également à raccorder les câbles à un tableau de connexions, une autre compétence essentielle pour l'installation de câbles.

Pour enfoncer les fils à l'intérieur de la prise, vous utiliserez un poinçon. Un poinçon est un outil à ressort qui sert à pousser les fils entre des broches métalliques tout en dénudant le fil. Ainsi, le fil établit une bonne connexion électrique avec les broches à l'intérieur de la prise. Le poinçon coupe aussi toute longueur de fil excédentaire.

Lorsque vous utilisez un poinçon, commencez par placer la lame à l'extérieur de la prise. Si vous placez la lame à l'intérieur de la prise, vous couperez le fil avant qu'il n'atteigne son point de contact. Dans ce cas, aucune connexion électrique n'est établie. (Remarque : Si vous inclinez le manche du poinçon un peu vers l'extérieur, il coupera mieux). Si des fils demeurent fixés après l'utilisation du poinçon, tournez délicatement leur extrémité pour les retirer, placez les pinces sur la prise et serrez-les.

Pour replacer la prise dans sa plaque, poussez la par l'arrière. Assurez-vous d'abord que la prise est dans le bon sens. Vissez ensuite la plaque au boîtier ou au support

Si le boîtier est monté en saillie, rappelez-vous qu'il peut contenir de 2,5 à 5 cm (1 à 2 po) de câble excédentaire. Vous devrez alors glisser le câble dans ses attaches ou tirer sur la canalisation qui le

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

recouvre afin de pousser le reste du câble à l'intérieur du mur. Si la prise est encastrée, vous n'avez qu'à pousser le câble excédentaire à l'intérieur du mur.

Démontrer l'installation des prises de courant et des prises RJ -45

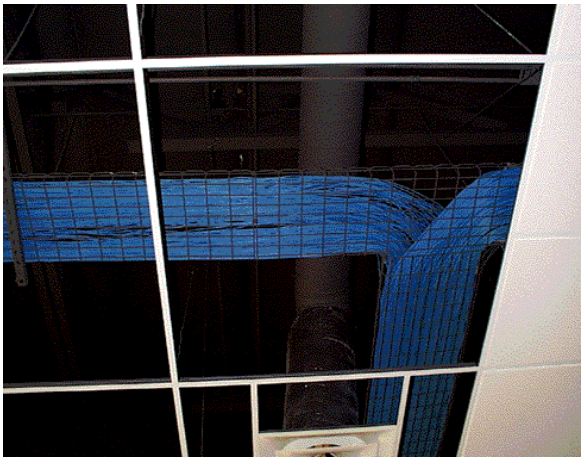
Note d'instructeur:
Cet objectif a simplement pour but de s'assurer que tous les étudiants ont vraiment exécuté les tâches des laboratoires.

Démontrez que vous savez encastrer une prise RJ45 dans du gypse, du plâtre et du bois. Démontrez également que vous savez raccorder et fixer des fils à une prise RJ45.

X-3- PRINCIPES FONDAMENTAUX DE L'INSTALLATION DES CABLES

Expliquer les principes de base de l'installation de câble à paires torsadées non blindées

Note d'instructeur:
Cet objectif traite des choses à faire et à ne pas faire pendant l'installation des câbles à paires torsadées non blindées. L'idéal est de faire la démonstration des méthodes recommandées et incorrectes pour que les étudiants comprennent bien la manipulation du câble.



Pour connecter des câbles aux prises, ne retirez que la longueur de gaine nécessaire pour établir la connexion. Plus le fil est dénudé, plus la connexion est faible et plus la perte de signal est élevée. Après avoir exposé les fils, assurez-vous que chaque paire de fils demeure torsadée, et ce, le plus près possible du point de raccordement. La torsade des fils permet l'annulation nécessaire pour éviter l'interférence électromagnétique et radio. Dans le cas des câbles à paires torsadées non blindées de catégorie 4, la longueur maximale permise de fil non torsadé est de 2,54 cm (1 po). Dans le cas des câbles à paires torsadées non blindées de catégorie 5, la longueur maximale permise de fil non torsadé est de 1,27 cm (1/2 po).

Si vous devez courber un câble au moment de l'acheminement, assurez-vous de maintenir un ratio de courbure quatre fois plus élevé que le diamètre du câble. Ne pliez jamais un câble à un angle supérieur à 90°. De plus, essayez de ne jamais étirer les câbles lorsque vous les manipulez. Si vous exercez une force de plus de 11,5 kg (25 livres) sur un câble, les fils à l'intérieur peuvent se détorsader ce qui, comme vous l'avez déjà appris, peut causer de l'interférence et de la diaphonie.

Si plusieurs câbles sont acheminés le long du même parcours, utilisez des attaches autoblocantes pour les regrouper. Placez-les à intervalles réguliers et serrez-les délicatement. Ne serrez pas les attaches trop fortement, elles peuvent endommager les câbles. Essayez, aussi, de minimiser la torsion des gaines des câbles. Si la torsion est trop forte, les gaines peuvent se déchirer. Les câbles ne devraient jamais être pincés ou entortillés. Si c'est le cas, le débit sera plus lent et la capacité du réseau local sera moins qu'optimale.

Avant tout, ne soyez jamais avare lorsque vous déterminez la longueur de câble nécessaire pour un parcours. Il est important de prévoir du câble excédentaire. Quelques mètres de câble supplémentaires est un bien petit prix à payer pour éviter de refaire un parcours de câble en raison de problèmes

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

d'étirement. La plupart des poseurs de câbles prévoient assez de câble supplémentaire pour que celui-ci atteigne le plancher et ils rajoutent ensuite un mètre (3 pi) à chaque extrémité. D'autres poseurs utilisent la méthode de l'*enroulement de service* qui consiste simplement à laisser quelques mètres de câble enroulés dans le plafond ou dans un autre emplacement hors de vue.

Utilisez des techniques appropriées et recommandées pour l'apprêt et la fixation des câbles, par exemple : attaches, supports, panneaux de gestion des fils et lanières de Velcro. N'utilisez jamais d'agrafes pour fixer des câbles. Les agrafes peuvent percer la gaine entraînant une perte de connexion.

Rappelez-vous des choses à faire et à ne pas faire relativement à l'installation des câbles.

Décrire la bonne méthode de documentation des parcours de câble

Note d'instructeur:
Les feuilles d'identification des câbles, les plans d'aménagement, les topologies physiques et logiques, les étiquettes de câbles et les entrées au journal ne sont que quelques-unes des techniques nécessaires pour bien documenter l'acheminement des câbles. Ne présentez pas la documentation comme une partie optionnelle de l'installation des câbles, mais bien comme une partie intégrante d'une installation professionnelle.

Pendant l'installation des câbles, il est important de documenter vos actions. Pour ce faire, utilisez une feuille d'identification des câbles pendant l'installation. Une feuille d'identification des câbles est un diagramme sommaire qui indique l'emplacement des parcours de câble. Elle indique également le numéro des classes, des bureaux ou autres salles où aboutissent les câbles. Plus tard, vous pourrez consulter cette feuille afin d'identifier les prises de télécommunications et les prises du tableau de connexions dans le local technique. Vous pouvez utiliser une page de votre journal pour documenter les parcours de câble. En consignant cette information dans votre journal, vous obtenez des renseignements supplémentaires pour toute installation de câbles.

Lister les spécifications de la norme EIA/TIA-606 concernant l'étiquetage des câbles

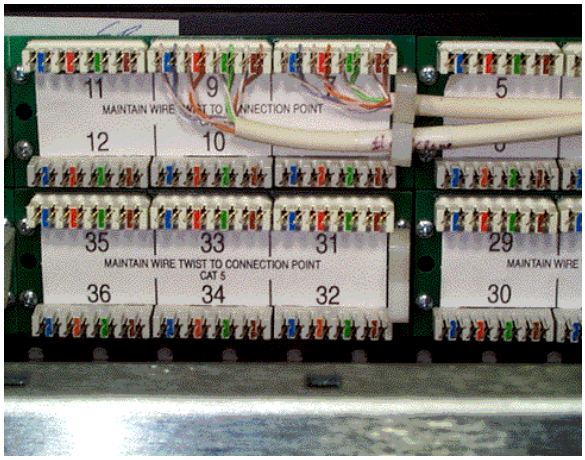
Note d'instructeur:
Soulignez l'importance (et la nécessité) de respecter les normes d'étiquetage des terminaisons de câbles (prises, tableaux de connexions, etc.).

La norme EIA/TIA-606 précise que chaque unité de raccordement doit être identifiée par un code unique. Cet identificateur doit être inscrit sur chaque unité de raccordement ou sur son étiquette. Lorsque des identificateurs sont utilisés dans la zone de travail, les raccordements de postes doivent être désignés par une étiquette sur la plaque, le boîtier ou le connecteur lui-même. Toutes les étiquettes, qu'elles soient collées ou insérées dans une pochette, doivent respecter les critères de lisibilité, de longévité et d'adhésivité précisés dans la norme UL969.

Décrire le genre d'étiquettes à utiliser

Note d'instructeur:
Il est essentiel d'utiliser un système d'étiquetage alphanumérique systématique pour les parcours de câbles et les terminaisons. En fin de projet, cette information devrait être consignée dans un chiffrier ou une base de données à des fins de référence et de maintenance.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com



Evitez d'étiqueter les câbles, les sorties de télécommunications et les tableaux de connexions avec des désignations comme «classe d'algèbre de M. Tremblay» ou «classe d'histoire de Mme Trudeau». Cela peut créer de la confusion, plusieurs années plus tard, si un technicien qui ne connaît pas ces désignations doit exécuter des travaux relatifs aux médias réseau. Utilisez plutôt des désignations qui demeureront compréhensibles à qui que ce soit plusieurs années plus tard.

Nombre d'administrateurs réseau incluent le numéro des salles dans les désignations. Ils attribuent des lettres à chacun des câbles aboutissant dans une salle. Certains systèmes d'étiquetage, particulièrement ceux des très grands réseaux, utilisent aussi le codage par couleurs. Par exemple, une étiquette bleue peut désigner un câblage horizontal dans le local technique seulement alors qu'une étiquette verte peut désigner un câble dans la zone de travail.

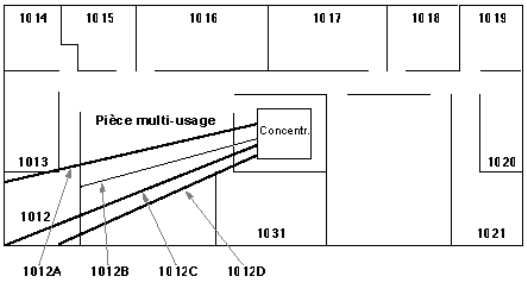


Diagramme d'identification des câbles

Étiquette de prise de télécommunications

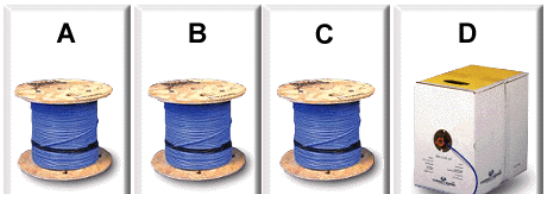
Pour illustrer ce concept, imaginez quatre câbles aboutissant à la salle 1012. Sur la feuille d'identification des câbles, ces câbles seraient désignés comme 1012A, 1012B, 1012C et 1012D. Les plaques où les câbles 1012A, 1012B, 1012C et 1012D sont reliés au cordons de connexion des postes de travail seraient aussi identifiées avec la désignation du câble correspondant.

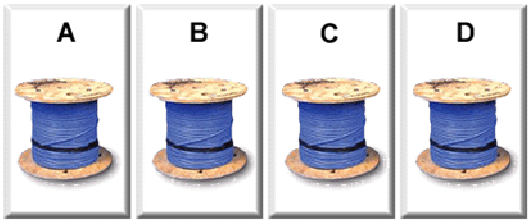
Chaque connexion de câble devrait aussi être étiquetée au tableau de connexions du local technique. Placez les connexions de sorte que les étiquettes soient en ordre croissant. Cela permet de poser des diagnostics et de localiser les incidents plus facilement le cas échéant. Finalement, étiquetez les câbles à chaque extrémité.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Décrire le processus de préparation des câbles pour l'inst allation et l'étiquetage

Note d'instructeur:
Une méthode efficace d'installation de plusieurs parcours de câbles est décrite.





Exemple : Après étude et analyse, il a été décidé d'acheminer quatre câbles à chacune des salles de votre école. Vous avez étudié le parcours des câbles du local technique aux salles de classe. Vous êtes maintenant prêt à acheminer les câbles.

Plutôt que d'acheminer séparément les quatre câbles le long du même parcours, il serait plus facile et plus rapide d'acheminer les quatre câbles simultanément. Pour ce faire, vous aurez besoin de quatre bobines de câble.

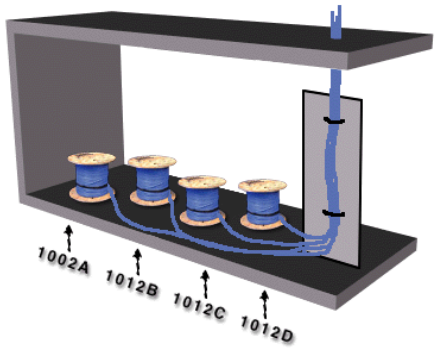
Chaque bobine contient 303 m (1 000 pi) de câble. Pour faciliter la manutention et éviter l'entortillage des câbles, les bobines sont généralement placées dans des boîtes. Le câble se déroule par un orifice dans le côté de la boîte pendant que la bobine tourne à l'intérieur. Si la bobine que vous utilisez se sépare de sa boîte, n'essayez pas de dérouler le câble. Le câble s'entortillerait. Plutôt, placez la bobine sur le cô té et déroulez le câble à mesure que vous en avez besoin. Cela empêchera le câble de s'entortiller et de s'emmêler. Pour vous aider à identifier les câbles qui se déroulent des bobines, attribuez une lettre à chaque bobine.

Placez les bobines au point central ou au local technique. Déroulez une courte longueur de câble de chaque bobine. Utilisez un marqueur permanent hydrofuge pour identifier l'extrémité de chaque câble de sorte qu'il corresponde à sa bobine. Dans notre exemple, vous savez que chaque câble sera acheminé à la classe 1012 alors inscrivez ce numéro devant chaque lettre. Une fois l'acheminement terminé, les câbles devraient être numérotés 1012A, 1012B, 1012C et 1012D. Pour vous assurer que les étiquettes ne seraient pas effacées ou coupées (à l' extrémité) plus tard, marquez le câble trois fois à environ 5 cm (2 po) d'intervalle.

Enroulez les câbles de ruban isolant pour les attacher ensemble. Attachez ensemble les extrémités des câbles et le bout d'une chaîne de tirage. Pour bien fixer la chaîne de tirage, nouez la chaîne de tirage autour des câbles avec des nœuds demiclef avant d'attacher les extrémités avec le ruban. Ne soyez pas avare de ruban. Si la chaîne ou les câbles se détachent ultérieurement, vous gaspillerez temps et argent.

Décrire quand et comment un câble est étiqueté à l'extrémité opposée

Instructor Note:
L'importance d'étiqueter les câbles à chaque extrémité est soulignée. L'importance d'étiqueter les câbles augmente rapidement en fonction du nombre de câbles à regrouper. Un éti quetage minutieux des câbles au moment de l'installation vous fera économiser beaucoup de temps et d'effort plus tard, au moment du dépannage.



Après avoir acheminé le câble le long du parcours déterminé plus tôt, amenez-le à la salle de classe. (Remarque : Une section ultérieure traitera de manière plus détaillée des techniques utilisées pour acheminer des câbles à l'intérieur des murs, le long des murs, à l'intérieur de greniers et

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

derrière les plafonds suspendus.) Prévoyez assez de câble pour que les ext rémités puissent atteindre les emplacements des prises, plus assez de câble excédentaire pour aller jusqu'au plancher plus un mètre supplémentaire.

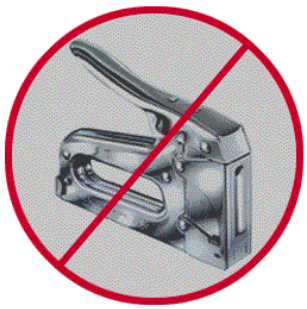
Retournez aux bobines de câble au point central ou local technique. Servez -vous des étiquettes sur chaque bobine comme référence et marquez chaque câble avec la lettre et le numéro de salle appropriés. Ne coupez pas les câbles avant qu'ils soient identifiés. Pour obtenir les meilleurs résultats, coupez les câbles et la chaîne de tirage avec des pinces à connexi ons. Cet outil permet de couper nettement les câbles sans perte de signal.

Si vous suivez chacune de ces étapes, les médias réseau servant au câblage horizontal seront étiquetés à chaque extrémité.

X-4- INSTALLATION DES PARCOURS DE CABLES STRUCTURES

Décrire la procédure la plus simple pour passer un câble

Note d'instructeur:
Plusieurs méthodes d'acheminement des câbles moins recommandées sont décrites. D'entrée de jeu, l'utilisation d'agrafes est inacceptable. L'utilisation de ruban adhésif étanche l'est également. Une méthode facile, bien que pas très esthétique, consiste à attacher les câbles ensemble au moyen d'attaches et de visser les attaches au mur.



La méthode la plus simple pour acheminer un câble est de le monter sur un mur. Toutefois, n'utilis ez cette méthode que si vous êtes certain que le câble ne sera pas bousculé ou tiraillé. Pensez à des emplacements où cette technique pourrait être utilisée.

Pour monter un câble au mur, vous devez choisir un dispositif qui le fixera au mur. Les attaches autoblocantes conviennent très bien. Si l'attache ne risque pas d'être déplacée, vous pouvez opter pour des attaches adhésives. Bien que ces attaches soient faciles à utiliser, rappelez -vous qu'elles ne peuvent pas être déplacées ultérieurement. S'il est probable que le câble sera déplacé plus tard, les attaches perforées sont un meilleur choix. Ce type d'attache est fixé au mur avec des vis.

Avant de fixer des vis dans un mur de maçonnerie, vous devez percer des trous dans le mur. Cela peut poser des problèmes. Si les trous doivent être d'un diamètre inférieur à 1 cm (3/8 po), vous pouvez utiliser une perceuse électrique munie d'une mèche au carbone. Prenez tout le temps nécessaire. Si les trous doivent être d'un diamètre supérieur à 1 cm (3/8 po), il y a de fortes chances que la perceuse électrique surchauffe. Cette tâche exigera un outil appelé marteau perforateur. Un marteau perforateur ressemble à une grosse perceuse électrique, mais contrairement à cette dernière, le marteau perforateur pique rapidement pendant que la mèche tourne. (Remarque : En appuyant le marteau perforateur fermement contre la surface à percer, vous pouvez augmenter son efficacité et la vitesse de perforation.)

N'utilisez jamais d'agrafes pour fixer des câbles à un mur. Vous souven ez-vous pourquoi? L'utilisation d'agrafes pour fixer des câbles n'est pas conforme à la norme EIA/TIA -568A.

Expliquer comment installer un câble dans une canalisation

Note d'instructeur:
Les canalisations et les gouttières sont présentées comme deux métho des privilégiées d'acheminement des câbles. Toutefois, ces méthodes ne sont pas économiques, les canalisations étant coûteuses, particulièrement si les parcours de câble sont longs.

Vous pouvez également acheminer les câbles en les passant dans une canali sation. Les canalisations sont des canaux muraux avec couvercle amovible. Il en existe deux types. Le premier type de canalisation est dit décoratif, car il présente une apparence plus finie. Les canalisations décoratives servent à camoufler les câbles le long d'un mur dans une pièce où ils seraient visibles autrement.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

L'autre type de canalisation porte le nom de gouttière. Comme son nom le laisse supposer, la gouttière est moins attrayante que la canalisation décorative. Son principal avantage, toutefois, est de pouvoir contenir plusieurs câbles. Règle générale, l'utilisation des gouttières est limitée aux endroits comme les greniers ou les espaces créés par les plafonds suspendus.

La canalisation peut être faite de métal ou de plastique et être montée à l'aide de vis ou collée grâce à un côté adhésif. Quel pourrait être un inconvénient possible d'une canalisation à endos adhésif? Quel pourrait être un avantage possible d'une canalisation à endos adhésif?

Une fois que la canalisation est installée, placez le câble à l'intérieur et fixez le couvercle. Cela protégera le câble.

Expliquer comment déterminer si un câble peut être passé dans une canalisation existante

Note d'instructeur:
Il faut généralement tenir compte de deux aspects avant d'acheminer un câb le dans une canalisation existante. Premièrement, y a-t-il de l'espace? Le nouveau faisceau de câbles que vous désirez acheminer dans la canalisation peut excéder la capacité de celle -ci. Deuxièmement, il est préférable de ne pas acheminer de câbles dans une canalisation contenant des fils électriques. Cela peut engendrer des problèmes de bruit.

Vous connaissez peut-être déjà les canalisations, car elles sont souvent utilisées pour d'autres genres de câble. Il n'est pas rare d'en trouver dans les immeubles où l'on installe ou étend des réseaux locaux. Dans de telles circonstances, les personnes chargées de l'installation se demandent si les câbles pourraient être acheminés dans les canalisations existantes. Cela dépend, en fait, du type de câble se trouvant déjà dans la canalisation.

Connaissez-vous un type de câble qu'il serait préférable de ne pas acheminer à côté d'un câble à paires torsadées non blindées de catégorie 5?

Enumérer les mesures de sécurité personnelle à prendre avant d'installer des câbles

Note d'instructeur:
Il s'agit, cette fois encore, d'une révision des mesures de sécurité. Ne vous lancez pas dans l'installation de câbles tant que vos étudiants ne sont pas suffisamment formés et mûrs, et sans supervision adulte suffisante. Il peut être très intéressant et enrichissant d'installer des câbles, mais comme il s'agit essentiellement de projets de construction, il faut prendre certaines précautions. Vous pourriez peut -être inviter quelques parents à vous aider lorsque vous réaliserez votre pro jet de câblage structuré; il est possible qu'il y en ait qui travaillent dans les domaines de la construction et de l'électricité.

Lorsque vous travaillez dans les murs, les plafonds ou les greniers, **la première chose à faire est de couper le courant alimentant tous les circuits qui pourraient passer dans** ces **zones de travail!** Si vous n'êtes pas certain si des fils traversent la section de l'édifice dans laquelle vous travaillez, **la règle d'or est de couper le courant partout**. **Ne touchez jamais, en aucun cas, aux câbles d'alimentation! Même si vous pensez avoir coupé tout le courant dans la zone où vous travaillerez,** il n'existe aucun moyen de savoir si ces câbles sont sous tension.

Avant de commencer à travailler, repérez l'emplacement de tous les extincte urs dans la zone. De plus, il est bon de se vêtir de manière appropriée. Les manches longues et les pantalons protègent les bras et les jambes. Evitez de porter des vêtements très amples ou bouffants. S'ils s'accrochent à quelque chose, vous pourriez être blessé.

Si vous prévoyez travailler dans un plafond suspendu, examinez d'abord la zone. Pour ce faire, soulevez quelques-uns des carreaux de plafond et regardez alentour. Vous pourrez ainsi repérer les conduits électriques, les conduits d'air, l'équipement mécanique et tout ce qui pourrait causer des problèmes plus tard.

Si vous devez utiliser des cisailles ou une scie, portez des lunettes de sécurité. Il est bon également de porter des lunettes de sécurité lorsque vous travaillez dans un vide sanitaire ou au-dessus d'un plafond suspendu. Si quelque chose tombe ou si vous vous appuyez sur quoi que ce soit dans le noir, vos yeux seront protégés.

Informez-vous auprès de l'ingénieur d'entretien de l'immeuble si la zone dans laquelle vous travaillerez contient de l'amiante, du plomb ou des PBC. Dans un tel cas, suivez la réglementation gouvernementale relative à ces matériaux.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Gardez votre zone de travail bien rangée. Ne laissez pas d'outils à des endroits où quelqu'un pourrait buter contre eux. Soyez prudents avec les outils munis de longs cordons prolongateurs. Tout comme les outils, les cordons peuvent facilement faire trébucher quelqu'un.

Enumérer les précautions à prendre pour assurer la sécurité de l'immeuble

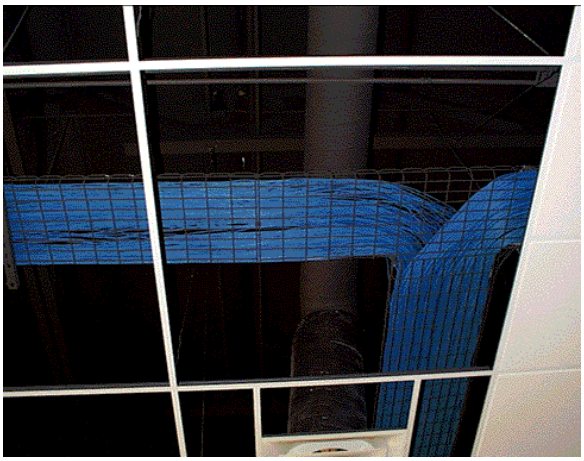
Note d'instructeur:
Les précautions à prendre ne touchent pas uniquement l'installateur et les autres personnes. Il faut aussi penser à l'immeuble.

Prenez toujours connaissance à l'avance des normes de construction locales. Certains codes de bâtiment peuvent interdire de percer ou de découper des trous dans les plafonds ou les murs coupe-feu. L'administrateur du site ou l'ingénieur des installations pourra vous aider à déterminer les zones interdites.

Si vous trouvez de l'isolant endommagé lors de l'installation de câbles, n'acheminez pas les câbles dans cette zone. Dans certaines situations, si vous percez un trou dans un mur, vous devrez le boucher complètement avec un produit de colmatage non combustible. Cette fois encore, l'ingénieur des installations pourra vous aider à identifier les endroits où cette précaution est nécessaire.

Enfin, si vous devez acheminer des câbles dans des endroits où une circulation de l'air est effectuée, vous devez utiliser un câble classé résistant au feu.

Décrire le processus de support du câblage horizontal dans un grenier ou une pièce avec plafond suspendu



Note d'instructeur:
Les options pour l'acheminement des câbles dans les plafonds suspendus sont présentées. La seule option inacceptable est de simplement déposer les câbles sur le plafond suspendu.

Beaucoup d'installateurs aiment bien acheminer les câbles par le grenier ou un plafond suspendu, car ils sont ainsi invisibles. Lorsque vous passez un câble dans un plafond suspendu, ne posez jamais le câble sur le plafond. Utilisez un autre support pour le câble.

Les gouttières murales, dont nous avons parlé plus tôt, sont un des moyens de supporter les câbles. Vous pouvez également utiliser les attaches servant à suspendre le plafond surbaissé pour fixer les câbles. Lorsque cette option est utilisée, le câble est simplement passé d'une attache à l'autre. Il existe également une troisième option pour supporter les câbles : le bâti en échelle. Les bâtis en échelle, qui sont suspendus au véritable plafond, offrent un support optimal pour les câbles.

Expliquer comment passer un câble dans un grenier ou une pièce avec plafond suspendu

Note d'instructeur:
L'utilité de la perche pour saisir les câbles dans des endroits difficiles d'accès est expliquée.

Les greniers et les zones au-dessus des plafonds suspendus peuvent s'avérer des endroits inconfortables, où il est difficile de travailler. Ce sont souvent des endroits sombres, poussiéreux, restreints et peu aérés. La température peut y monter en flèche, surtout durant l'été.

Une perche apporte une solution simple et facile à ces problèmes. La perche est en fait une tige télescopique munie d'un crochet à une extrémité afin de retenir le câble. Elle permet de faire traverser rapidement un câble dans un plafond suspendu ou un grenier.

Expliquer comment tirer un câble depuis le dessus d'un mur

Note d'instructeur:
Description de la façon de passer les câbles dans les murs à l'aide de ruban de tirage.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Lorsque vous devez tirer un câble dans un mur depuis le grenier ou l'espace créé par un plafond suspendu, il vous faut d'abord repérer la sablière du mur et y percer un trou de ¾ po. Descendez ensuite lentement le ruban de tirage dans le mur, par le trou que vous venez de percer. Demandez à une autre personne de se placer près de l'ouverture dans le mur, sous l'endroit où vous êtes . Demandez à votre assistant de vous avertir lorsque le crochet du ruban de tirage atteint l'ouverture dans le mur. L'assistant doit alors saisir le ruban de tirage.

Il doit dénuder le câble à paires torsadées non blindées de catégorie 5 sur environ 2,5 cm . Ensuite, il doit replier les fils autour du crochet du ruban de tirage et les fixer à l'aide de ruban isolant. Vous pouvez alors tirer le câble dans le mur jusqu'à la sablière. Laissez suffisamment de câble à la prise pour qu'il touche le sol, plus un autre 60 à 90 cm.

Expliquer comment tirer un câble depuis le bas d'un mur

Note d'instructeur:
Description de la manière de tirer un câble par -dessous un mur (dans le cas d'un accès par le sous -sol).

Pour acheminer horizontalement les câbles dans un immeuble ayant un sous-sol, vous pouvez les amener dans les autres zones de travail au rez-de-chaussée à partir du sous-sol. Pour ce faire, vous devez d'abord percer un trou de 1/8 po en angle dans le plancher tout près de la plinthe. Passez un cintre ou un fil rigide dans le trou pour marquer l'endroit lorsque vous serez dans le sous -sol.

Allez au sous-sol et repérez le cintre ou le fil. A l'aide d'un ruban à mesurer, faites une marque sous le mur, à 2 ¼ po du trou. Percez un nouveau trou de ¾ po de diamètre à ce t endroit. Contrairement au premier trou qui était percé en angle, percez celui -ci verticalement dans le sous-plancher et la sablière. Vous devriez alors pouvoir pousser le câble par ce second trou jusqu'à l'ouverture dans le mur où la prise sera installée. Laissez suffisamment de câble pour qu'il touche le sol, plus un autre 60 à 90 cm.

X-5- PASSAGE ET MONTAGE DES CABLES

Démontrer votre habileté à accomplir ces tâches

Note d'instructeur:
En vous servant d'un faux mur, d'un endroit dans l'immeuble ou de l 'emplacement réel de votre projet de câblage structuré, demandez aux étudiants de démontrer les compétences acquises relativement au passage, à l'acheminement et à la pose des câbles.

Démontrez les techniques suivantes :

. Tirer le câble du bas vers le haut .
. Tirer le câble du haut vers le bas.
. Passer un câble dans un plafond suspendu.
. Fixer un câble au mur à l'aide d'attaches.
. Fixer un câble au mur à l'aide d'une canalisation décorative.
. Fixer un câble au mur à l'aide d'une gouttière.
. Installer un câble à l'aide d'un bâti en échelle.
. Passer un câble au moyen d'une perche.
. Passer un câble au moyen de ruban de tirage.
o. Passer un câble au moyen d'une chaîne de tirage.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

X-6- PRINCIPES FONDAMENTAUX DES LOCAUX TECHNIQUES ET DES TABLEAUX DE CONNEXIONS

Définir local technique

Note d'instructeur:
Révision des locaux techniques

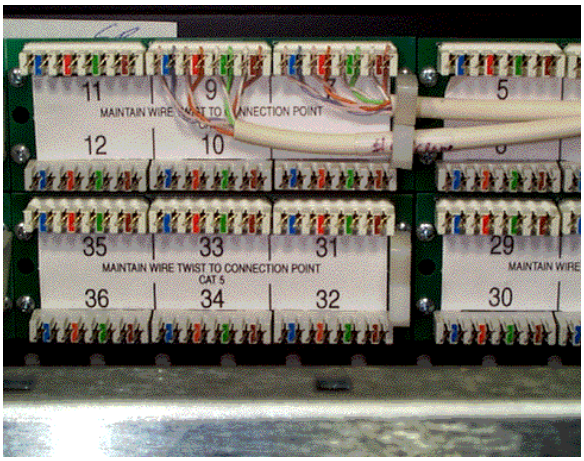
Un local technique est une pièce spécialement conçue comme point de jonction central du câblage et de l'équipement de câblage servant à connecter les unités d'un réseau local. C'est le point central d'une topologie en étoile. Habituellement, le local technique contient des tableaux de connexions, des concentrateurs de câblage, des ponts, des commutateurs et des routeurs.

Indiquer si un réseau peut être doté de plus d'un local technique

Note d'instructeur:
Révision des notions relatives aux répartiteurs principaux et secondaires

Les grands réseaux comptent parfois plus d'un local technique. Dans ce cas, un des locaux techniques est habituellement désigné comme *répartiteur principal*. Tous les autres, appelés *répartiteurs intermédiaires*, en dépendent. Une telle topologie porte le nom de topologie en étoile étendue.

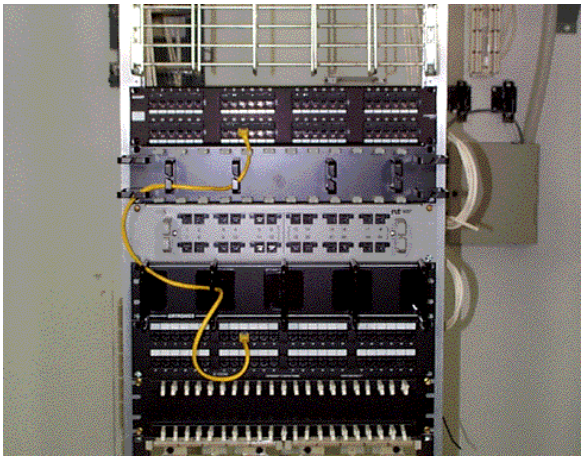
Préciser à quoi sont connectés les parcours de câblage horizontal dans le local technique



Note d'instructeur:
Présentation de la structure et de l'importance des tableaux de connexions. Il pourrait être utile de faire circuler des tableaux de connexions non montés, si vous en avez, pour que les étudiants puissent les examiner.

Dans un réseau local Ethernet à topologie en étoile, les parcours de câbles horizontaux provenant des zones de travail sont habituellement raccordés à un tableau de connexions. Un tableau de connexions est un dispositif d'interconnexion par l'intermédiaire duquel les parcours de câbles horizontaux peuvent être connectés à d'autres dispositifs de réseautage, comme des concentrateurs et des répéteurs.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com



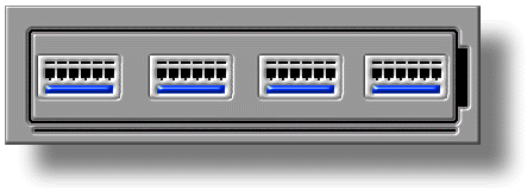
travail pour former un réseau local.

Dans certains cas, le tableau de connexions peut aussi permettre à des unités de se connecter à un réseau longue distance ou à Internet. Cette connexion est décrite par la norme EIA/TIA-568A comme une *interconnexion horizontale*.

Plus précisément, un tableau de connexions est un ensemble de ports et d'emplacements de broches. Le tableau de connexions joue le rôle d'une matrice reliant les câbles horizontaux des postes de travail à d'autres postes de

Décrire la structure d'un tableau de connexions

Note d'instructeur:
Rappelez aux étudiants que l'arrière du tableau de connexions est construit comme l'arrière des prises RJ -45, qu'ils connaissent déjà.



Ports à l'avant d'un tableau de connexions

Pour comprendre comment un tableau de connexions permet d'interconnecter les câbles horizontaux à d'autres dispositifs de réseautage, examinons sa structure. Un côté du tableau de connexions comporte des rangées de broches chromocodées, tout comme celles d'une prise RJ-45.

Pour effectuer les connexions électriques aux broches, vous devez utiliser un poinçon pour enfoncer les fils. N'oubliez que l'ordre des fils est primordial pour des performances réseau optimales. Par conséquent, lorsque vous connectez les fils au tableau de connexions, assurez-vous que la couleur des fils correspond à celle des broches. Les couleurs des fils et des broches ne sont pas interchangeables.

De l'autre côté du tableau de connexions se trouvent les p orts. Ces ports ressemblent à ceux des prises de télécommunications de la zone de travail. Les ports du tableau de connexions exigent des fiches de même taille que les ports RJ-45. Il est possible d'interconnecter des ordinateurs et d'autres dispositifs réseau (ex. : concentrateurs, répéteurs et routeurs) également reliés au tableau de connexions, grâce à des cordons de raccordement qui se branchent sur ses ports.

Décrire comment les fils sont disposés au tableau de connexions

Note d'instructeur:
Rappelez aux étudiants qu'ils doivent poser les fils sur le tableau de connexions comme ils ont procédé pour les prises RJ-45. Il est important de ne pas détorsader les fils de plus de ½ po, ce qui peut être difficile si l'étudiant n'est pas minutieux.

Dans tout réseau local, les points les plus faibles sont les connecteurs. S'ils ne sont pas bien installés, les connecteurs peuvent engendrer du bruit électrique et causer des contacts électriques intermittents

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

entre les fils et les broches. Lorsque cela se produit, la transmission des données dans le réseau est perturbée ou se déroule à un débit nettement inférieur. Il vaut donc la peine de faire les choses comme il faut. Pour être bien certain que le câble est installé correctement, suivez les normes EIA/TIA.

Au tableau de connexions, posez les fils des câbles en ordre croissant, par numéro de câble. Aidez-vous de la feuille d'identification des câbles que vous avez préparée plus tôt. Vous pourrez ajouter les étiquettes plus tard. Utilisez les numéros qui ont été attribués au moment de l'acheminement des câbles de la zone de travail au local technique. Les numéros de câble devraient correspondre aux numéros des bureaux où sont situés les postes de travail. Si vous disposez les câbles en ordre croissant au tableau de connexions, il sera beaucoup plus facile de repérer et de diagnostiquer les problèmes futurs.

Pendant la pose des fils, il est important de maintenir les extrémités des câbles centrées au-dessus des emplacements de broches. Si vous n'êtes pas consciencieux, les fils peuvent se tordre, ce qui ralentira le débit de transmission des données une fois le réseau entièrement raccordé.

Assurez-vous de laisser la gaine jusqu'à 0,62 cm (1/4 po) des emplacements de broches sur lesquels vous travaillez afin de ne pas exposer trop de fil. Pour ce faire, prenez le temps de mesurer avant de dénuder les fils - 3,75 à 5 cm (1 1/2 à 2 po) devraient suffire. Si vous dénudez trop les fils, il en résulte un débit de transmission des données plus lent. N'oubliez pas non plus de ne pas défaire les torsades des paires de fils plus qu'il n'est nécessaire. Les fils détorsadés transmettent les données plus lentement et peuvent être cause de diaphonie.

Décrire comment les fils sont connectés au tableau de connexions

Note d'instructeur:
Rappelez aux étudiants qu'ils savent déjà comment utiliser un poinçon grâce à leurs travaux sur les prises RJ -45 et que les mêmes procédures s'appliquent aux tableaux de connexions.

Le type de tableau de connexions détermine s'il faut utiliser un poinçon *110* ou *Krone*. Le tableau illustré dans ce chapitre est de type 110. Vérifiez de quel poinçon vous avez besoin avant de commencer à travailler.

Un poinçon est un outil à ressort de rappel. Cela lui permet de remplir deux fonctions à la fois. En effet, tout en enfonçant un fil entre deux broches métalliques et en le dénudant (afin d'établir une connexion électrique avec les broches), le poinçon coupe aussi le fil en trop. Il arrive parfois que le poinçon ne fasse pas une coupe nette. Dans ce cas, tournez doucement les extrémités coupées et retirez-les une fois que le fil a été mis en place.

Lorsque vous utilisez le poinçon, assurez-vous de le placer de sorte que la lame soit opposée au point où le fil est enfoncé dans chaque emplacement de broche. Sans cette précaution, vous pourriez couper le fil trop court par rapport à son point de connexion électrique.

Expliquer comment monter un tableau de connexions

Note d'instructeur:
Présentation du montage des tableaux de connexions sur des supports, dans des bâtis et des armoires. Insistez sur le fait que tout cela vise à structurer le câblage afin qu'il soit facile à gérer.

Vous pouvez monter les tableaux de connexions au mur à l'aide de supports ou les placer dans des bâtis ou des armoires (équipées de bâtis et de portes). L'une des pièces d'équipement les plus courantes est le *bâti de distribution*. Il s'agit en fait d'une charpente renfermant de l'équipement utilisé dans le local technique, notamment des tableaux de connexions, des répéteurs, des concentrateurs et des routeurs. Le bâti de distribution peut mesurer de 1 m à 1, 9 m de hauteur.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

L'avantage du bâti de distribution est qu'il permet d'accéder facilement à l'avant comme à l'arrière de l'équipement. Pour en assurer la stabilité, le bâti de distribution est fixé au plancher au moyen d'une plaque de plancher. Bien que quelques entreprises commercialisent un bâti de 0,58 m (23 po) de largeur, c'est le modèle de 0,48 m (19 po) qui est le plus répandu depuis les années 1940.

X-7- EQUIPEMENT UTILISE POUR TESTER LES PROJETS DE CABLAGE STRUCTURE

Décrire la procédure pour tester les câbles déjà installés

Note d'instructeur:
Présentation d'un modèle de dépannage simple pour l'essai des câbles. La couche 1 étant à la source de bon nombre de problèmes de réseau, tout professionnel en réseautage doit pouvoir effectuer le dépannage au niveau de la couche 1.

Vous savez maintenant que le média de réseautage constitue le fondement du modèle OSI et que chacune des autres couches dépend du média de réseautage ou est pris e en charge par celui-ci. Vous avez également appris qu'un réseau ne peut être plus fiable que son câblage. En fait, de nombreux experts le considèrent comme le composant le plus important d'un réseau.

Il est donc important de déterminer la qualité de l'i nstallation une fois que le média de réseautage a été installé. Malgré le fait qu'il puisse être constitué de câbles, de connecteurs, de tableaux de connexions et d'autres équipements de la meilleure qualité, de mauvaises pratiques d'installation peuvent e mpêcher un réseau de fonctionner à son niveau optimal. Lorsque tout est en place, l'ensemble de l'installation doit être mis à l'essai.

Pour tester votre réseau, suivez les étapes ci-dessous :

. Découpez le système en éléments fonctionnels logiques.
. Notez tous les symptômes.
o. Servez-vous des symptômes pour déterminer l'élément le plus susceptible d'un mauvais fonctionnement.

§ Effectuez une substitution ou des essais supplémentaires pour vérifier si l'élément le plus probable est vraiment celui qui ne fonctionne pas correctement.
§ Passez au deuxième élément le plus probable si le premier s'est avéré en bon état de marche.
§ Réparez l'élément défectueux dès que vous le trouvez.
§ Remplacez-le si vous ne pouvez pas le réparer.

Expliquer comment savoir si un réseau fonctionne correctement

Note d'instructeur :
Explication de l'importance d'une mesure de référence des performances d'un réseau. Cette mesure de référence ou de base est constituée d'un ensemble de données au sujet du réseau, que vous vérifiez périodiq uement pour vous assurer que le réseau fonctionne toujours comme il le devrait.

L'IEEE et l'EIA/TIA ont établi des normes qui vous permettent de vérifier si votre réseau fonctionne à un niveau acceptable. Si votre réseau réussit ce test et est confirmé co nforme aux normes, vous pouvez utiliser cette mesure comme référence.

Il est important de connaître la mesure de référence. La conformité aux normes de l'installation ne signifie pas la fin des tests pour autant. Vous devez continuer à effectuer des vérif ications périodiques pour vous assurer que le réseau fonctionne toujours à son meilleur. Pour cela, vous pouvez comparer les mesures actuelles aux mesures enregistrées, prises lorsque le système fonctionnait bien. S'il y a une différence importante par rap port à la mesure de référence, c'est une indication que quelque chose ne va pas.

En effectuant des vérifications répétées du réseau et en comparant les résultats à la mesure de référence, vous pourrez plus facilement détecter des problèmes particuliers et suivre la dégradation causée par le vieillissement, de mauvaises pratiques de maintenance, la température ou d'autres facteurs.

Décrire tout équipement spécial ou toute formation nécessaire pour tester des câbles

Note d'instructeur:

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Cette section insiste sur l'importance d'un équipement spécialisé de vérification des câbles.

Vous pensez peut-être que pour vérifier un câble, il suffit de lui en substituer un autre. Cela ne prouve rien de façon certaine, car un problème commun pourrait affecter tous les câbles d'un réseau local.

Pour cette raison, il est recommandé d'utiliser un testeur de câbles pour mesurer les performances du réseau. Un testeur de câbles est un dispositif portatif capable de certifier qu'un câble répond aux normes de l'IEEE et de l'EIA/TIA. Les fonctions offertes par les testeurs de câbles varient selon le type de testeur. Certains fournissent des imprimés, d'autres peuvent se connecter à un PC pour créer un fichier de données.

Aucune formation spéciale n'est nécessaire pour utiliser les testeurs de câbles disponibles sur le marché de nos jours. La plupart des administrateurs réseau ou des installateurs compétents considèrent que les guides d'utilisation fournis par les fabricants suffisent amplement.

Définir les testeurs de câble et indiquer ce qu'ils mesurent

Note d'instructeur:
Présentation de certains paramètres de base mesurés par les testeurs de câbles. Un exemple de câblomètre est le Fluke 620 (ou l'équivalent), qui peut déterminer la continuité et la configuration des broches, identifier les câbles, en calculer la longueur, repérer les mauvaises connexions, fournir des schémas des fils pour la détection des paires inversées, détecter les paires séparées et suivre les câbles derrière les murs.

Les testeurs de câbles présentent un large éventail de fonctions et de caractéristiques. La liste qui suit vous donne un aperçu des fonctions offertes. Vous devez déterminer quelles fonctions répondent le mieux à vos besoins avant de faire un choix.

Les testeurs de câbles peuvent effectuer des tests qui mesurent la capacité globale d'un parcours de câble. Exemples :

- déterminer la longueur du câble
- repérer les mauvaises connexions
- fournir des schémas de câblage pour détecter les paires inversées
- mesurer l'atténuation du signal
- mesurer la diaphonie locale
- détecter les paires séparées
- effectuer des vérifications du niveau de bruit
- suivre le tracé des câbles derrière les murs

Décrire comment un testeur de câble mesure la distance

Note d'instructeur:
Description des mesures de distance à l'aide d'un réflectomètre. Ce dispositif envoie une impulsion et attend le retour de sa réflexion; sachant le débit auquel les signaux traversent un média particulier (qui peut être mesuré et calculé, et qui est entré dans le réflectomètre par le fabricant), il calcule la distance à l'aide de la formule distance = le débit par le temps. La moitié du temps écoulé est le temps de propagation de l'impulsion dans le câble, qui donne la longueur du câble lorsqu'il est multiplié par la vitesse de propagation du signal. Vous pourriez comparer cet appareil à un radar de câble

Il est important de mesurer la longueur totale des parcours de câble, car la distance peut nuire à la capacité des unités du réseau de partager le média de réseautage. Ainsi que vous l'avez déjà appris, un câble dont la longueur dépasse le maximum précisé par la norme EIA/TIA -568A peut engendrer une dégradation du signal.

Les testeurs de câbles, parfois appelés *réflectomètres (TDR)*, mesurent la distance jusqu'à un câble en court-circuit ou à une extrémité non raccordée. Pour cela, ils envoient une impulsion électrique dans le câble. Ils calculent ensuite le temps que prend la réflexion du signal depuis l'extrémité du câble. Ce test appelé *réflectométrie dans le domaine temporel* peut donner des lectures de distance à 60 cm près (2 pi).

Expliquer comment utiliser les mesures de distance pour déterminer si les connexions aux prises de télécommunication et aux tableaux de connexions sont bonnes

Note d'instructeur:

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Cette section traite de l'utilité des mesures de distance pour vérifier la connectivité des prises, parcours de câble et tableau de connexions.

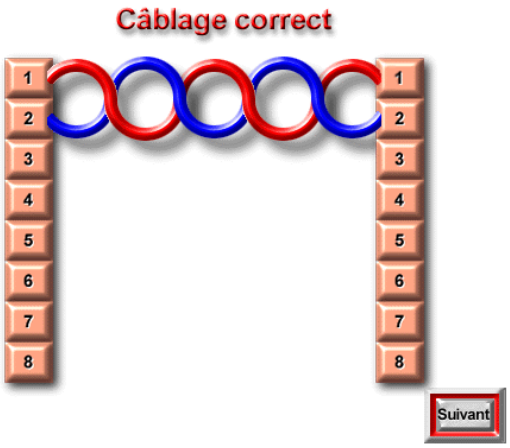
Dans les réseaux locaux utilisant des câbles à paires torsadées non blindées, les mesures de distance permettent de déterminer si les connexions aux tableaux de connexions et aux prises de télécommunications sont bonnes. Pour comprendre comment cela fonctionne, vous devez d'abord comprendre le fonctionnement d'un réflectomètre.

Le réflectomètre mesure la longueur d'un câble en envoyant un signal électrique dans le câble. Le signal est réfléchi lorsqu'il arrive à la connexion ouverte la plus éloignée. Pour identifier les connexions défectueuses sur un parcours de câble, vous devez connecter le réflectomètre au cordon de raccordement du tableau de connexions. Si le réflectomètre indique la distance jusqu'au tableau de connexions au lieu de celle à un point plus éloigné, vous savez immédiatement qu'il y a un problème de connexion.

Vous pouvez employer la même procédure à l'extrémité opposée du câble pour mesurer la distance jusqu'à la prise RJ-45.

Expliquer comment un testeur de câble peut détecter si l'installateur a inversé les fils à une prise

Note d'instructeur:
Cette section explique les paires inversées, une erreur de câblage fréquente.

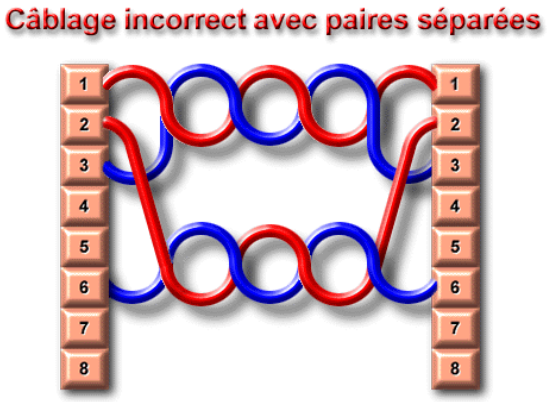


Les testeurs de câbles utilisent une fonction appelée *schéma de câblage* pour indiquer quelles paires de fils se connectent à quelles broches des bornes et prises. Le test indique si l'installateur a bien raccordé les fils d'une prise ou s'il les a inversés. Lorsque les fils sont dans l'ordre inverse, on parle alors de *paires inversées*. Il s'agit d'un problème courant, particulier aux câbles à paires torsadées non blindées.

Lorsque des paires inversées sont détectées dans les systèmes de câblage d'un réseau local à câbles à paires torsadées non blindées, cela signifie que les connexions sont mauvaises et qu'elles doivent être refaites.

Expliquer pourquoi un schéma de câblage ne permettra pas de détecter les paires séparées

Note d'instructeur:
Les appareils simples de mappage des fils ne détecteront pas les paires dont les fils sont séparés; cette opération requiert un appareil plus perfectionné.



L'inspection visuelle et les mesures de diaphonie sont les seules façons de détecter une situation connue sous le nom de *paires séparées*. Comme vous le savez, les torsades dans les paires de fils servent à protéger ces derniers des interférences extérieures causées par des signaux passant le long d'autres paires. Cependant, cet effet d'écran protecteur existe uniquement si les fils d'une paire font partie du même circuit. Lorsque les fils sont séparés, ils ne font plus partie du même circuit. Même si le courant passe dans le circuit, donnant ainsi l'impression que le système fonctionne, il n'y a aucune protection. Les signaux ne sont donc pas protégés. Tôt ou tard, la diaphonie locale deviendra un problème. Un schéma de câblage ne peut pas détecter une situation de paire séparée parce qu'il y a quand même un circuit.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Décrire comment un testeur de câble mesure l'atténuation du signal

Note d'instructeur:
Règle générale, il faut utiliser un testeur de câbles plutôt cher (plus de 1 000 $) pour effectuer des tests d'atténuation du signal. Ces mesures sont décrites. Un de ces dispositifs est le Fluke DSP -2000.

Divers facteurs peuvent diminuer la puissance d'un signal passant dans les fils de cuivre d'un câble à paires torsadées non blindées. Cette réduction de la puissance du signal s'appelle *atténuation*. Elle se produit lorsqu'un signal (impulsions représentant des bits de données) perd de l'énergie au profit du câble. Un testeur de câbles permet de mesurer la diminution de la puissance d'un signal provenant d'un dispositif d'injection de signaux (petite boîte de la taille d'un jeu de cartes connectée à l'extrémité éloignée d'un câble). Habituellement, les testeurs de câbles mesurent l'atténuation à diverses fréquences. Dans le cas des câbles à paires torsadées non blindées de catégorie 5, les testeurs de câbles peuvent prendre des mesures à des fréquences allant jusqu'à 100 MHz.

Vérifiez les spécifications EIA/TIA 568A pour connaître l'affaiblissement permis pour le type de câble utilisé dans votre réseau local.

Identifier les causes de la diaphonie locale

Note d'instructeur:
Règle générale, il faut utiliser un testeur de câbles plutôt cher (plus de 1 000 $) pour effectuer des tests de diaphonie locale (NEXT). Ces mesures sont décrites. Un de ces dispositifs est le Fluke DSP -2000.

Plusieurs facteurs peuvent contribuer à la *diaphonie locale*. Le plus courant est la présence de paires inversées. Comme vous l'avez vu précédemment, celles-ci peuvent être détectées au moyen de la fonction de schéma de câblage d'un testeur de câbles.

La diaphonie locale peut aussi être causée par des paires qui ont été détorsadées au moment de leur raccordement à des dispositifs d'interconnexion comme des tableaux de connexions, par des cordons de raccordement détorsadés ou par des câbles trop tendus autour de coins aigus, ce qui provoque un changement de position des paires dans la gaine du câble. Si vous mesurez de la diaphonie locale, effectuez une vérification visuelle du câblage horizontal afin d'éliminer ces possibilités. Si vous ne trouvez rien, cela signifie que le problème est probablement dû à des paires séparées.

Un testeur de câbles vérifie la diaphonie locale en prenant des mesures à diverses fréquences allant jusqu'à 100 MHz. Les nombres élevés sont un bon signe; les petits nombres indiquent des problèmes dans le réseau.

Décrire les types de problème qu'un test du niveau de bruit permet de détecter

Note d'instructeur:
Présentation de la liste des principales sources de bruit.

De nombreux facteurs extérieurs peuvent causer de l'interférence dans le média de réseautage. Voici quelques exemples de sources externes qui émettent des signaux a yant un effet sur les paires de fils du câble à paires torsadées non blindées :

- éclairage fluorescent
- appareils de chauffage
- radios
- purificateurs d'air
- téléviseurs
- ordinateurs
- détecteurs de mouvement
- radar
- moteurs
- commutateurs
- soudeuses
- démarreurs automatiques
- appareils électroniques de toutes sortes

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Heureusement, les signaux produits par ces sources externes utilisent souvent des fréquences particulières. Ceci permet donc à la vérification du niveau de bruit de détecter non seulement une telle interférence extérieure, mais aussi de réduire les sources d'émission possibles.

Expliquer comment un testeur de câble peut repérer les sources d'interférences externes

Note d'instructeur:
Règle générale, il faut utiliser un testeur de câbles plutôt cher (plus de 1 000 $) pour effectuer des tests du niveau de bruit. Ces mesures sont décrites. Un de ces dispositifs est le Fluke DSP -2000.

Avant d'utiliser un testeur de câbles pour prendre des lectures du bruit dans un câble, déconnectez tous les câbles de l'équipement informatique. Des niveaux de lecture élevés indiquent généralement un problème. Un moyen simple de repérer la source précise du bruit consiste à débrancher chacun des dispositifs électriques jusqu'à ce que vous la trouviez. Sachez toutefois qu e cela ne fonctionne pas toujours.

Mettre en pratique les procédures de test des câbles

Note d'instructeur:
Les étudiants doivent démontrer qu'ils sont capables d'utiliser des testeurs simples de la continuité des câbles. Le professeur doit au moins faire la démonstration d'un Fluke 620 ou l'équivalent pour la vérification des câbles. Si d'autres appareils Fluke (ou équivalents) sont disponibles, vous augmenterez les compétences professionnelles des étudiants en les formant à utiliser ces appareils. Si vou s disposez de testeurs de câbles haut de gamme (prêtés par l'institut régional ou une entreprise locale d'installation de câbles), faites -en la démonstration, ce sont vraiment des dispositifs remarquables qui mesurent bon nombre des paramètres traités dans le cadre de ce programme d'études.

Votre professeur fera la démonstration de quelques-unes des vérifications que l'on peut effectuer à l'aide d'un testeur de câbles. Dans certains cas, ces vérifications dénoteront un problème. Vous devrez expliquer brièvement comment déterminer la nature du problème et décrirez ce qu'il faut faire pour le corriger.

Pendant la deuxième partie du laboratoire, vous devrez démontrer que vous pouvez utiliser une topologie en étoile pour réaliser un réseau local Ethernet simple. Votre professeur évaluera votre capacité à manipuler le câble correctement, à poser et à connecter les fils dans une prise et dans un tableau de connexions, afin de réaliser de bonnes connexions.

Une fois que vous aurez raccordé votre réseau local à topologie en étoile, il vous faudra le vérifier. Si les tests indiquent des problèmes, vous devrez les diagnostiquer et les corriger. Cette série d'exercices en laboratoire vise à réaliser un réseau local à topologie en étoile entièrement fonctionnel et conforme aux spécifications EIA/TIA et IEEE.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

EXERCICES SUR LA MAINTENANCE DU CABLAGE

Cet exercice est à réaliser en atelier.

Objectif de l'exercice :

- **A l'aide d'instruments de mesure et d'utilitaires, vérifier l'installation du laboratoire de réseautique 5 11 109**

Vous avez à votre disposition les outils suivants :

- Instruments de mesure
  - Testeur de câble Fluke
  - Analyseur de câble Fluke DSP2000
- Utilitaires
  - Moniteur réseau (Windows 2000 serveur)
  - Analyseur de performance
  - Gestionnaire de périphérique
  - Utilitaire de maintenance pour PC (Sandra, ou Dr Hardware 2000
  - Utilitaire de diagnostic de la carte réseau.

Travail demandé

L'exercice doit être réalisé en atelier. Veuillez faire vérifier votre travail par le professeur pour vous assurer que vous obtenez votre marque de participation.

1. Vérification du câblage du réseau (inspection visuelle) Reproduire les schémas.

- Brochage du câble direct
- Brochage du câble console (paires inversées)
- Brochage du câble croisé
- Documentation du réseau existant :
  - Schéma
  - numéro de la norme EIA TIA mise en application selon le code de couleur que vous avez discerné
  - nom des standards de réseau utilisé (exemple 10base T)
  - Type de connecteur utilisé (avec 2 ou 3 dents?)
  - Type de câble utilisé (monobrin ou multibrin quelle catégorie)

2. Test du câblage de catégorie 5

Vérification du câblage, de la prise PC au panneau d'interconnexion, avec les instruments de mesures

Mesures à faire	Résultat obtenu
Numéro de circuit	
Résultats des test	
NEXT (para diaphonie	
Résistance	
Longueur	
Atténuation	
…	

3. Analyse du trafic à l'aide de l'analyseur de câble (optionnel)

Cette activité est optionnelle. Si vous souhaitez utiliser les fonctions avancées de l'analyseur de câble vous pouvez tracer des graphiques de l'activité du réseau et des graphiques des résultats obtenus au point 2. Veuillez consulter le professeur qui vous expliquera les étapes principales.

Vous pouvez consulter aussi les extraits du manuel du DSP 2000 qui vous sera remis.

Pages 2.7, 2.8 2.12, 2.13, 2..15 3.2, à 3.19 4.9 à 4.20, 5.1 à 5.5, 7.1 à 7.26 8.12 à 8.13, B1 à B9

4. Vérification de la carte interface réseau

Il ne faut pas changer les réglages de la carte

4.1 Trouvez et reportez ci dessous les informations suivantes :

Interruptions	

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

ports d'entrée/sortie	
mémoire RAM d'échange	
Mode de fonctionnement (half ou Full Duplex)	

4.2 Tester le bon fonctionnement de la carte avec l'utilitaire de la carte fournit par le fabricant de la carte. Cet utilitaire ne vous est pas fournit. C'est à vous de le trouver. Il est important de réaliser ce test dans les conditions prescrites par le fabricant. (machine ayant démarré sous DOS sans réseau).

4.3 Configurez et utilisez l'analyseur de performance pour obtenir des informations sur la carte réseau. Vous pouvez utiliser l'aide en ligne de Windows pour voir comment configurer le moniteur réseau. Nous utiliserons cet utilitaire fréquemment dans le cadre du cours.

- Octets envoyés par seconde
- Octets perdus
- Paquets reçus avec erreur
- Veuillez produire un journal de conteurs appelé Network.tsv (format texte délimité. Avec quel utilitaire pouvez vous le consulter?
- Voici comment avoir un diagnostic de son réseau

Comment avoir un diagnostic complet de votre réseau ?
- Ouvrir le menu démarrage, aller dans exécuter et taper : helpctr.exe pour XP ou winmsd pour windows 2000
- Ensuite dans la partie **"Choisissez une tâche"** (pour XP)
- cliquer sur :**"Utilisez Outils pour afficher les informations concernant votre ordinateur et diagnostiquer les problèmes"**
- Utilisez les fonctions appropriées pour la partie réseau . Le professeur fera une démo à l'écran.

5. Amélioration des performances réseau au niveau de la carte

Proposez quelques suggestions (suggestion www.winguides.com. « trucamichel » ou tweakUI) pour améliorer les performance de la carte réseau.

- a.
- b.
- c.

Reportez vos résultats dans le porte folio électronique module 2

Vous devez faire vérifier votre travail par le professeur à la fin de l'exercice (Point de participation).

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

PROJET DE CONCEPTION D'UN RESEAU INFORMATIQUE

Objectifs

Le projet doit permettre à l'étudiant d'effectuer toutes les étapes en vue de réaliser un réseau informatique en utilisant toutes les notions qu'il possède.

Etapes de réalisation

Le projet comprend les étapes suivantes :

. définition du projet
. analyse, recherche et planification de la solution
. implantation du réseau
. planification de la gestion et de l'administration du réseau
. planification d'une politique de sécurité

Pour chacune de ces étapes, les étudiants devront présenter un rapport. Ce rapport d'étape contiendra les éléments suivants :

- page titre, numéro de l'équipe, nom des équipiers et identification de l'étape
- table des matières
- compte rendu de l'étape
- suivi de la planification
- références

Chaque fin d'étape donnera lieue à une rencontre d'évaluation de l'équipe avec son professeur attitré, à qui sera remis le rapport.
Chaque rapport sera noté sur 6 points pour un total de 30 points

Les étudiants travailleront en équipe de 2 personnes, pour simuler le plus réalistement possible le marché du travail.

Définition du projet

La première étape du projet consiste à définir le projet qui devra respecter les normes suivantes :

Ø utilisation maximale des ressources mises à votre disposition
Ø utilisation exhaustive des notions apprises dans les cours du programme
Ø implantation et démonstration d'une application concrète sur le réseau
Ø complexité du réseau
Ø la réalisation du projet doit comporter au moins un élément d'innovation
Ø documentation

L'évaluation du projet

. **Rapports d'étape**

- méthodologie de réalisation du projet
  - o planification des étapes
  - o méthodes pour solutionner les problèmes
  - o professionnalisme et respect des échéanciers
- Contenu du rapport
  - o Quantité et qualité des informations contenues
  - o Respect des critères

2. Projet

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

- démonstration de l'application sur le réseau
  - complexité de l'application et de la mise en réseau
  - préparation et fonctionnalité de l'application
- gestion et administration du réseau
  - planification de l'administration du réseau
  - technique de gestion des tâches et des priorités
  - documentation des opérations
- sécurité du réseau
  - plan de secours (en cas de sinistre)
  - politique des copies de sécurité
  - contrôle des accès et sécurité des données
  - documentation des problèmes
- complexité et originalité du projet
  - quantité de notions développées dans le projet
  - innovations

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

CONTROLE CONTINU N° 3

Conception d'un réseau local commuté

Durée prévue : 60 min

Objectifs :

- Analyser les exigences pour un réseau local simple avec accès à Internet.
- Concevoir une topologie de couche 1 et 2 pour un réseau Ethernet commuté et les exigences données
- Déterminer le type, le nombre et l'emplacement de commutateurs Ethernet et des câbles nécessaires, selon l'emplacement des locaux techniques du répartiteur principal et des répartiteurs intermédiaires, à partir d'un plan d'étage simple
- S'informer au sujet des modèles et des prix sur les sites de Cisco et de ses fournisseurs

Contexte :

Ce laboratoire vous aidera à vous préparer pour l'étude de cas. Dans ce laboratoire, vous avez les exigences de base pour un petit réseau local qui s'étend sur plusieurs édifices. Vous devez vous concentrer sur la topologie physique et les composantes de la couche Liaison de données. L'objectif est de remplacer un ancien réseau Ethernet Thinnet 10BASE2 par le câblage et les commutateurs de la technologie Ethernet la plus récente en suivant les normes de câblage structurées avec une topologie en étoile étendue. Vous allez choisir quel type de commutateurs Ethernet utiliser et leurs emplacements. Vous allez également sélectionner le type de câble en fonction des exigences données. Vos utilisateurs auront besoin d'accéder à plusieurs serveurs, dont l'emplacement sera choisi pour une efficacité optimale. Vous vous servirez de catalogues des fournisseurs et d'informations sur le Web pour trouver les numéros de modèles et estimer les coûts des diverses solutions de commutation Ethernet.

Outils et préparation :

Il s'agit d'un laboratoire de recherche qui ne demande aucune installation particulière. Vous devrez avoir accès aux catalogues d'équipements de communication de données et au Web pour faire vos recherches. Utilisez les URL du site Web de Cisco donnés ci-dessous. Formez des groupes de travail de trois ou plus. Avant de commencer ce laboratoire, vous devriez lire le chapitre 4 sur la conception de réseau local du manuel "Networking Academy Second Year Companion Guide". Vous devriez aussi revoir le chapitre 4 en ligne de la troisième session. L'équipement nécessaire est énuméré ci-dessous.

- PC avec accès à Internet pour faire des recherches sur les produits
- Catalogues des fournisseurs d'équipements de communication de données

Notes :

_____

_____

_____

_____

_____

Etape 1. Revoir les exigences

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Vous allez concevoir le réseau local d'une petite entreprise avec un site et plusieurs édifices qui ont besoin d'être interconnectés. Utilisez le plan de l'édifice et les exigences pour déterminer l'endroit où doit être installé chaque type de commutateurs, ainsi que le tracé des différents câbles.

. Le campus de l'entreprise se compose de tro is édifices : administration, ingénierie et fabrication.

. L'édifice A est celui de l'administration, l'édifice B, de l'ingénierie et l'édifice C, de la fabrication.

. L'immeuble administratif se trouve entre les deux autres.

. Les distances entre les immeubl es sont indiquées sur le diagramme.

. Chacun des immeubles possède son local technique.

. Le local technique du point de présence se trouve dans l'immeuble administratif.

. Dans l'édifice administratif, 35 PC et 5 imprimantes doivent accéder au réseau.

. Dans l'édifice d'ingénierie, 27 PC et 3 imprimantes doivent accéder au réseau.

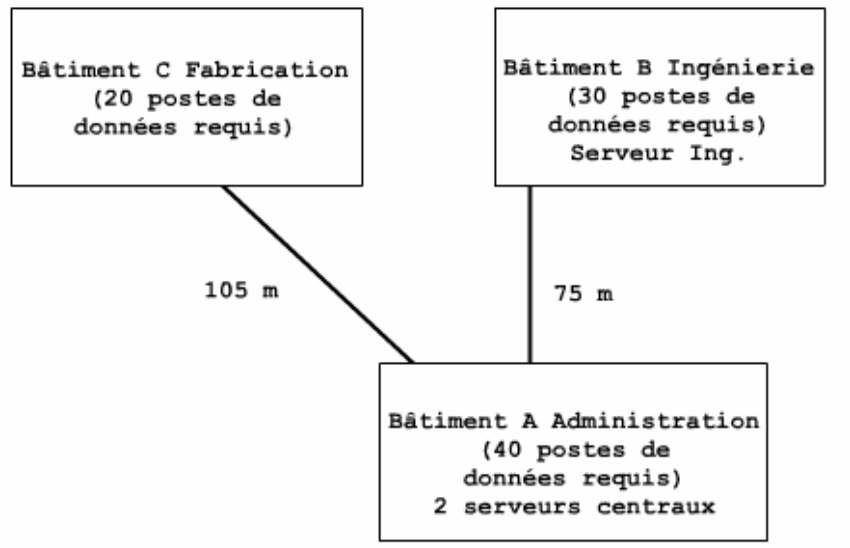
. Dans l'édifice de fabrication, 18 PC et 2 imprimantes doivent accéder au réseau.

a. Le client veut la technologie de commutation Ethernet la plus rapide pour le réseau primaire.

a. Il souhaite également réduire les coûts de connexion des postes de travail.

l . Les utilisateurs doivent avoir accès à Internet, à deux serveurs de fichiers et d'impressions centralisés.

Les utilisateurs de l'ingénierie doivent pouvoir accéder localement à un se rveur hautes performances.



Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Réseau de données de la société XYZ

Remplissez le tableau et répondez aux questions suivantes d'après vos connaissances sur les équipements de commutation Ethernet, les routeurs et les normes de câblage structuré.

. **Edifice administratif A - Equipement du répartiteur principal et du point de présence (40 données)**

Type d'équip.	Modèle	Qté	No/type ports	Description et fonction :	Coût

. **Edifice d'ingénierie B - Equipement du répartiteur intermédiaire 1 (30 données)**

Type d'équip.	Modèle	Qté	No/type ports	Description et fonction :	Coût
			(1)		

. **Edifice de fabrication C - Equipement du répartiteur intermédiaire 2 (20 données)**

Type d'équip.	Modèle	Qté	No/type ports	Description et fonction :	Coût

. Quel type de câblage utiliserez-vous pour relier les commutateurs du local technique aux postes de travail des utilisateurs? Justifiez votre choix.

. Quelle sera la vitesse de ces liens?

. Quels termes sont liés à ce type de câblage?

. Quel type de câblage utiliserez-vous pour relier le répartiteur principal ou le point de présence de l'immeuble A aux immeubles B et C? Justifiez votre choix.

. Quelle sera la vitesse de ces liens?

. Quels termes sont liés à ce type de câblage?

h. Pourquoi le local technique de l'immeuble administratif est-il le meilleur endroit pour installer le répartiteur principal?

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

XI- STRATEGIE DE DEPANNAGE DES RESEAUX

XI-1- IDENTIFIER LES CHANGEMENTS INTERVENUS SUR LE RESEAU

Les réseaux donnent parfois l'impression que des gremlins se cachent dans chaque serveur, dans chaque câble, et surtout dans chaque PC fonctionnant sous Windows 95. Pourtant, très souvent, ce qu'on pourrait être tenté d'attribuer à des gremlins est en fait la conséquence d'une modification effectuée par un être humain, qui a simplement oublié (ou qui refuse de' reconnaître) ensuite qu'il a effectué cette modification.

Nous commettons tous cette erreur ; nous sommes notre pire ennemi. A titre d'exemple, supposez que vous veniez d'installer un nouveau navigateur. Or, ce nouveau logiciel ne vous convient pas, et vous décidez de le supprimer du disque dur de votre ordinateur. Cependant, dès le lendemain, vous rencontrez des problèmes pour vous connecter à l'Intranet de votre entreprise. Si vous avez de la chance ou de la mémoire, vous vous souviendrez peut-être que vous avez installé ce nouveau navigateur la veille, et vous pourrez sans doute vous en sortir en le réinstallant. Toutefois, que se passera-t-il si un week-end entiers'écoule entre cette installation malheureuse et l'apparition de vos problèmes d'accès ? Vous risquez de perdre des heures à réfléchir aux raisons qui peuvent vous empêcher de vous connecter.

Le syndrome de la main maladroite

Le même principe s'applique quand vous intervenez sur un serveur ou un routeur. Supposez que vous veniez d'effectuer une modification sur un serveur ou sur un routeur pour offrir un nouveau se rvice ou pour réparer un problème. Si la modification porte ses fruits, elle risque d'être le dernier élément que vous penserez à incriminer si un nouveau problème apparaît un peu plus tard. Supposez que vous constatiez que le fichier de démarrage de votr e serveur IntranetWare ne rend pas un certain volume systématiquement disponible. Vous essayez de remédier au problème en éditant le fichier de démarrage. Le jour-même, les utilisateurs de Windows NT - et non de Windows 95 - viennent se plaindre que leur horloge est décalée de cinq heures. Y aurait-il un lien avec la modification que vous venez d'effectuer ? Impossible ! Cela doit venir de la configuration de Windows NT, non ? Cela ne peut pas venir du serveur.

Et pourtant, c'est bel et bien du serveur que vient le problème. En réfléchissant bien, vous constatez que vous êtes une nouvelle fois victime du syndrome de la main maladroite, c'est-à-dire que vous avez modifié l'un des fichiers de configuration (si mineure qu'ait été la modification), vous avez in séré par erreur un caractère ou deux qui ont rendu une commande ou un paramètre inintelligibles pour le serveur. Dans ce cas précis, le problème s'est produit quand vous avez modifié le fichier de démarrage d'IntranetWare pour régler un problème bénin. Vous avez appuyé par erreur sur une touche qui a modifié la partie supérieure du fichier. En examinant ce fichier, vous constatez que la première ligne de ce fichier sert en fait à définir le fuseau horaire.

Au lieu d'indiquer SET TIME ZONE=EST5EDT

vous constatez que cette ligne indique \SET TIME ZONE=EST5EDT

Quand vous avez enregistré le fichier de démarrage après avoir résolu le "problème bénin", le serveur n'était plus en mesure de savoir quel fuseau horaire utiliser. En effet, un serveur ne peut pas comprendre la commande \set. Comme les ordinateurs Windows NT connectés à l'aide d'un produit Novell synchronisent leur heure sur l'heure du serveur et utilisent beaucoup les fuseaux horaires, votre "main maladroite" a provoqué un décalage horaire de cinq heures. Aïe!

Conclusion : remettez-vous toujours en question quand un nouveau problème apparaît. Demandez-vous toujours ce que vous venez de faire, et soyez prêt à annuler les modifications à peine effectuées. Comme cela a été indiqué dans le chapitre pr écédent, si vous consignez dans un journal de bord les opérations que vous effectuez sur le réseau, il vous sera plus facile de déceler l'origine d'un problème.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Arme de votre journal de bord, vous pourrez comparer la date d'apparition du problème aux diffé rentes dates auxquelles vous êtes intervenu sur le réseau.

Bien entendu, d'autres personnes peuvent également avoir leur part de responsabilité, surtout si vous n'êtes pas le seul à vous occuper du réseau. Là encore, il est extrêmement utile de tenir un journal de bord. Toutefois, ne vous cantonnez pas à ce journal ; utilisez-le comme support pour discuter avec vos collaborateurs des problèmes que pose le réseau et des modifications que chacun d'entre.vous a effectuées.

ASTUCE

Avant de commencer à résoudre un problème, allez voir les utilisateurs du réseau et vos collaborateurs, et demandez-leur s'ils ont effectué la moindre modification.
Il est particulièrement difficile de résoudre un problème provoqué par une "main maladroite" quand la personne fautive n'a pas réinitialisé immédiatement l'ordinateur ou le périphérique sur lesquels elle est intervenue. Quand le périphérique ou l'ordinateur sont enfin réinitiali ses, la modification n'est plus récente et il est donc difficile de la mettre en cause. Conséque nce logique de ce qui précède, si vous rencontrez un problème alors qu'un périphérique vient d'être réinitialisé, vous pouvez parfaitement supposer que c'est au niveau de ce périphérique que se situe le problème.

ASTUCE

D'une manière générale, quand vous modifiez un périphérique, réinitialisez-le juste après la modification. Toutefois, cette règle n'est pas imparable. En effet, supposez qu'une autre personne soit intervenue sur le réseau qu'elle ait eu la main maladroite. Au terme de son intervention, la pe rsonne n'a pas réinitialisé le périphérique qu'elle a modifié. Quand vous intervenez à votre tour, vous réinitialisez le périphérique que vous venez de modifier dans les règles de l'art, et c'est alors que, contre toute attente, un nouveau problème apparaît. Vous pouvez lutter contre ce type de problème en réinitia lisant systématiquement les périphériques avant d'intervenir dessus. Ainsi, vous vous assurez que le périphérique à modifier fonctionne parfaitement.

Consultants et sous-traitants pas de confiance aveugle !

Le consultant que vous avez engagé pour prendre en charge votre réseau a certainement à coeur de satisfaire tous vos désirs, mais il est également tenu de respecter son emploi du temps. Il n'aime pas effectuer plus de travail que celui pour lequel il a été payé, et il a tout intérêt à vous vendre en permanence de nouveaux produits et services. Par ailleurs, il est probablement impliqué dans plusieurs projets simultanément ; il peut surgir à tout moment sur le pas de votre porte, ce qui n'est p as nécessairement très pratique pour vous. Vous pouvez exiger de lui qu'il apporte à votre réseau les modifications que vous souhaitez quand vous le souhaitez. Après tout, laisseriez-vous votre plombier libre d'aller et venir dans votre maison à tout momen t afin de régler votre chauffe-eau ?

Pour les projets de grande ampleur, exigez que le contrat comprenne une clause de remise en état d'origine en cas de problème. Cette clause se révélera très utile si vous estimez que le consultant a occasionné un préju dice en intervenant sur votre réseau, c'est-à-dire si les choses vont plus mal après son passage qu'avant. Vous devez évaluer le coût de la remise en état d'origine en termes de temps et d'argent. A titre d'exem ple, si vous avez décidé de convertir un ser veur Windows NT en serveur IntranetWare ou UNIX, il faudra qu'un technicien, intervienne sur chaque station de travail. Si vous devez ensuite annuler cette conversion, il faudra beaucoup de temps, et l'opération vous coûtera donc très cher. Comme le consul tant peut vous demander, après coup, de prendre en charge vous-même le coût de la remise en état d'origine, il est préférable de prévoir dès le départ une clause spécifique dans le contrat pour tous les projets d'une certaine ampleur. Le prix d'une prestat ion consistant à installer de nouveaux produit et à les désinstal 1er s'ils ne fonctionnent pas peut être sensiblement différent du prix d'une prestation consistant à tout installer, puis à "voir s'il y a moyen de résoudre le problème en cas de dysfonctionnement". Avant de conclure un contrat, veillez à vous protéger. De plus, si vous vous adressez à un consultant réputé pour son professionnalisme, il ne devrait pas sourciller si vous abordez des considérations de ce type pendant la phase de négociation.

INFO

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Ne vous laissez pas intimider par votre consultant, mais ne vous comportez pas non plus en dictateur envers lui. Il pourra devenir une aide très précieuse pour tous vos problèmes de dépannage, ou au contraire une source de problèmes si vos rapports avec lui se détériorent. Evidemment, la première hypothèse est la plus souhaitable pour vous.

Problèmes liés à des partenaires extérieurs

Deux types de partenaires n'ont même pas besoin d'entrer dans les locaux de votre entreprise pour vous causer des soucis : votre fournisseur d'accès, qui vous permet de surfer sur le Web, ainsi que d'envoyer et de recevoir des messages électroniques, et la compagnie de télécommunica tions qui vous permet peut-être de connecter vos sites les uns aux autres par l'intermédiai re de liaisons louées. De ces deux partenaires, la compa gnie de télécommunications est de loin la plus mature. Bien que les compagnies de. télécommunications aient toujours suscité des critiques exacerbées de la part du public, elles connaissent généralement bien leur métier, qu'elles exercent depuis plusieurs dizaines d'années, et tendent à mettre en oeuvre des stratégies efficaces pour s'adapter au change ment. Les fournisseurs d'accès, en revanche, n'existent que depuis cinq ou six ans, et il est facile de voir qu'ils souffrent toujours d'une certaine immaturité.

Le lundi est parfois un jour très éprouvant. Les fournisseurs d'accès et les compagnies de télécommunications profitent généralement du week-end, période où les utilisateurs sont les moins nombreux, pour modifier leurs infrastructures. Si quelque chose qui fonctionnait le vendredi ne fonctionne plus le lundi, il est temps de prendre votre télé phone et d'appeler votre fournisseur d'accès pour lui demander ce qui a changé. Il est probable qu'il v ous réponde "rien", mais si vous pouvez vérifier que rien n'est tombé en panne durant le week-end et si vous ne savez pas où chercher, le problème peut parfaitement disparaître mystérieusement pendant le déjeuner.

Pour les problèmes plus durables, vous ri squez d'avoir à convaincre votre fournisseur d'accès que votre matériel informatique fonctionne parfaitement, et que ce sont donc ses infrastructures qui sont en cause. Vous pouvez également découvrir que, finalement, votre réseau présente un problème, auq uel cas vous devrez vous préparer à présenter vos excuses a votre fournisseur d'accès. Pour vous assurer du bon fonctionnement de votre matériel, vous pouvez mettre en place un réseau de test. Si deux sites ne parviennent pas à communiquer ensemble, vous pouvez également rassembler votre matériel sur un même site et connecter directement les différents composants. Une fois la vérifica tion faite que votre matériel fonctionne, vous serez en mesure de prou ver à votre fournisseur d'accès que votre matériel e st parfaitement fonctionnel et que quelque chose a nécessairement changé entre les deux sites.

Le rapport risques/avantages

Il est toujours intéressant de disposer de nouveaux programmes. Ils offrent de nouvelles fonctions inexistantes sur les programmes plus anciens, et il est toujours valorisant d'être le premier à avoir la dernière version de tel ou tel logiciel. Cependant, l'expérience montre que chaque nouvelle version d'un logiciel apporte en moyenne deux nouveaux bogues. La course au développement à laquelle les éditeurs de logiciels se livrent sur l'Internet fait peser une pression insoutenable sur les développeurs, qui doivent absolument être les premiers sur le marché. Il s'ensuit que la période de test des produits est généralement écourtée, ce qui signifie que les programmes sont souvent commerciali sés avec quelques bogues. Consultez régulièrement le site Web des éditeurs de logiciels ; vous y trouverez des patchs pour les produits qui sont sur le marché depuis au moins six mois.

Comme vous avez mieux à faire que de passer votre journée à signaler aux éditeurs de logiciels les problèmes que vous rencontrez avec leurs produits, le mieux est de ne pas être le premier à installer une nouvelle application ou un nouveau système d'exploitation sur vot re réseau. A moins d'avoir absolument besoin des nouvelles fonctions qu'offre un logiciel, attendez toujours six mois après la sortie d'un logiciel pour l'essayer. Si vous avez vraiment besoin d'installer un nouveau logiciel avant ce délai, prenez en consi dération le rapport risques/avantages. Vous évaluerez ainsi les avantages que vous pensez retirer de cette installation, rapportés aux risques que vous encourez si l'opération ne se déroule pas correctement.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Une fois la décision prise d'utiliser un nouveau produit, vous devez encore vous assurer que vous n'allez pas rencontrer des problèmes en l'utilisant. A titre d'exemple, quand Windows 95 est sorti, beaucoup de services d'informatique ont commencé à l'utiliser en interne pendant un an avant d'autoriser les autres membres de leur entreprise à l'utiliser. (Bien entendu, l'installation d'un nouveau système d'exploitation entraîne une multitude de changements ; dans la pratique, il est peu probable que vous soyez prêt à attendre un an pour généraliser l'utilisation d'un nouveau traitement de texte ou d'un nouveau tableur au sein de votre entreprise.) Au cours de la phase de test d'un produit, il est primordial de l'essayer dans un environnement de production limité. En d'autres termes, il faut l'installer sur un petit nombre d'ordinateurs, sur lesquels les utilisateurs s'en serviront pour leur travail quotidien, et voir comment les choses se passent. Si tout se déroule correctement, vous pouvez, en principe, généraliser l'utilisation du nouveau produit à l'ensemble de votre entreprise. Si vous rencontrez des problèmes, au contraire, il sera aisé de remettre les ordinateurs dans leur état d'origine puisque vous n'en aurez modifié qu'un petit nombre.

Il est important que le déploiement du nouveau produit soit progressif. En d'autres termes, une fois qu'un logiciel a fait ses preuves avec un petit nombre d'employés, vous pouvez le configurer pour un nombre d'utilisateurs de plus en plus important, au lieu de le mettre d'emblée à la disposition de tous les utilisateurs. Vous mettrez tous les atouts de votre côté en déployant tout d'abord votre nouveau produit au sein de petits groupes d'utilisateurs, puis en laissant ces petits groupes grossir quand vous aurez constaté que tout se déroule correctement. Vous pouvez, par exemple, laisser cinq personnes accéder à une nouvelle application. Ensuite, si l'application fait ses preuves, vous pouvez en autoriser l'accès à dix personnes supplémentaires par semaine, puis quinze, puis vingt, etc. Lors de la dernière phase du déploiement (une fois que vous êtes certain que tout se passe correctement), vous pouvez mettre l'application à la disposition de trente personnes supplémentaires par semaine. Grâce à ce déploiement progressif, si vous rencontrez un problème au début de la phase de test, peu de personnes seront affectées.

Même si vous ne rencontrez pas de problème direct durant la phase de test d'un périphérique ou d'un logiciel, ceux-ci peuvent avoir des effets secondaires qui ne semblent pas liés au nouvel élément. Aussi est-il vivement conseillé de toujours éteindre, ou désactiver, les composants de réseau qui viennent d'être installés quand vient le moment de résoudre des problèmes de réseau ou de communication. Le problème n'est pas nécessairement provoqué par le nouveau périphérique ou le nouveau programme que vous venez d'installer, mais en désactivant ou en désinstallant le nouvel élément, vous pourrez avoir la certitude qu'il n'est pas à incriminer.

Si le problème disparaît, vous pouvez vous adresser au revendeur (ou au fabricant) auquel vous avez acheté le nouveau produit. Toutefois, vérifiez que le problème est reproductible (vous devez pouvoir faire réapparaître le problème en réinstallant le programme ou le périphérique incriminé) avant de contacter votre revendeur.

Donnez un maximum d'informations à votre revendeur, surtout si vous passez par un service d'assistance technique en ligne. Ainsi, le technicien qui s'occupera de votre problème sera en mesure de recréer votre environnement de travail dans son atelier. Une fois encore, les journaux de bord et les rapports d'incidents sont extrêmement utiles pour dépanner un réseau - de surcroît, les services d'assistance technique semblent plus disposés à solliciter leurs cellules grises quand les problèmes leur sont soumis par écrit.

XI-2- DIVISER POUR REGNER

Alors que Napoléon venait de s'autoproclamer empereur, Beethoven aurait modifié la dédicace de sa *Symphonie héroïque*, en l'honneur de Bonaparte, pour écrire "à la mémoire d'un grand héros". Restons modeste : l'objectif n'est pas de faire de vous un Napoléon du dépannage de réseaux, mais la stratégie consistant à diviser pour régner va néanmoins faire de vous un grand dépanneur. Elle a fonctionné pour Napoléon et il n'y a pas de raison qu'elle ne fonctionne pas pour vous.

Mais que peut bien vouloir dire "diviser pour régner" dans le contexte d'un réseau ? Tout simplement que pour résoudre un problème, il est plus facile de le diviser en problèmes plus petits. Quand vous savez qu'un problème affecte une zone donnée (un segment de réseau, ou des PC configurés d'une

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

certaine manière, par exemple), vous pouvez déterminer précisément la source du problème en divisant la zone incriminée en plusieurs zones.

INFO

Neuf fois sur dix, un seul problème sévit sur un réseau à un moment donné. Si votre parc informatique n'a pas été frappé par la foudre récemment, il est extrêmement improbable que vous soyez confronté à plusieurs problèmes simultanément (ce qui ne signifie pas qu'il n'existe pas d'effets d'entraînement en matière de dépannage de réseaux).

Le jeu du plus ou moins

Puisque, en principe, un seul problème peut se poser à la fois, il est relativement facile d'en identifier la cause (même sur un réseau de grande taille). Supposez qu'un passant vous demande de deviner un nombre compris entre un et un million. Si vous procédez séquentiellement, vous risquez de devoir proposer tous les nombres possibles. Vous pouvez donc avoir à proposer 999 999 nombres avant de trouver celui que le passant a en tête. Toutefois, si vous divisez chaque fois le nombre maximal en deux pour proposer une valeur et si le passant répond à vos propositions par "plus" ou "moins" afin de vous aiguiller, vous n'aurez besoin que de 23 propositions (au maximum). pour découvrir le nombre. Voilà une amélioration substantielle ! Vous êtes sceptique ? Alors, prenons un exemple

Le passant : Bon, j'ai en tête un nombre compris entre 1 et 1 000 000. A vous de le deviner.

Vous : 500 000 ?

Le passant : Non, moins !

Vous : 250 000 ?

Le passant : Non, plus !

Vous : *(après avoir marqué une pause pour calculer 250 000/2 + 250 000)* 375 000 ?

Le passant : Non, moins !

Vous : (devenant fou à l'idée de devoir deviner ce nombre compris entre 250 000 et 375 000) Voyons, il y a 125 000 nombres entre 250 000 et 375 000 ; le nombre du milieu doit être... euh... 312 500 ?

Le passant : Non, moins !

Vous : *(sortant votre calculatrice)* 281 500 ?

Le passant : Non, moins !

1/bus : *(tombant directement sur le bon nombre grâce à votre chance insolente) 265 625 ?*

Le passant : *(étonné) Oui !* Comment avez-vous deviné ?,

En réalité, il vous faudrait probablement quelques propositions supplémentaires pour deviner vraiment le nombre que le passant a en tête, mais l'idée est là : à l'origine, la plage de valeurs possibles est de 1 000 000 de valeurs, ce qui est gigantesque. Ensuite, elle n'est plus que de 500 000, puis de 250 000, puis de 125 000, puis de 62 500, puis de 31 250, puis de 15 625, puis de 7 812, etc. Comme vous pouvez le voir, le nombre de zéros diminue relativement rapidement en quelques propositions. Au bout de la septième proposition, il ne reste plus que 60 possibilités. Rassurez-vous, tout cela ne relève pas de la magie, mais de la logique. La Figure 4.1 montre le gain de temps que permet d'obtenir une division systématique par deux d'une zone de réseau qui pose problème.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

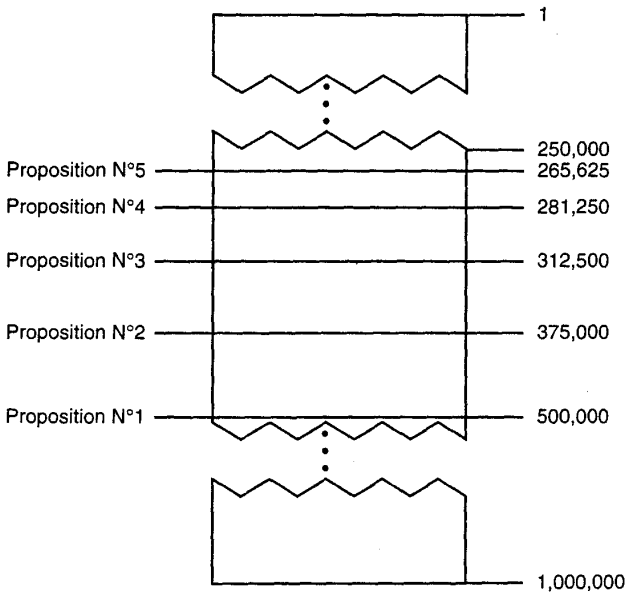


Figure 4.1
Dans une recherche binaire, la zone de recherche devient de plus en plus réduite au fur et à mesure que le nombre de propositions augmente.

INFO
Si vous souhaitez impressionner votre chef de service ou faire sensation à une réunion, vous pouvez présenter cette méthode sous le nom de recherche binaire. En prime, vous pouvez griffonner sa représentation mathématique sur le transparent du rétroprojecteur
n=log2 (x)
Ici, x est le nombre maximal de la séquence, et n est le nombre maximal de propositions possibles.

Votre Waterloo : le. réseau est en panne !
Voyons maintenant comment vous devez procéder quand le réseau est en panne. Tout d'abord, comment se présente la panne ? Y aurait-il un problème physique ? Un routeur ou un serveur auraient-ils un problème ? Votre stratégie pour faire face à ce type de situation : diviser pour régner. Quand vous êtes confronté à un problème, faites appel à votre sens logique, et partez de l'ensemble de votre réseau (la plage de nombres de 1 à 1 000 000) pour arriver au problème précis (le nombre 265 625). Vous devez probablement commencer par déterminer si le problème n'affecte qu'une personne (auquel cas il s'agit d'un problème local), ou au contraire tout un groupe de personnes (auquel cas il s'agit d'un problème systémique).

Si vous aboutissez à la conclusion qu'une seule personne est concernée, vous pouvez mettre au placard, temporairement, votre méthode consistant à diviser pour régner, et vous attaquer au dépannage de la station de travail incriminée. (Ce dépannage peut nécessiter de combiner différentes techniques, et notamment de diviser pour régner.) Si non, si plusieurs personnes sont affectées par le problème, vous devez rassembler davantage d'informations. Tous les utilisateurs sont-ils privés de réseau ? Généralement, la réponse est "non" !

INFO
En fait, il peut arriver que tous les utilisateurs soient privés de réseau, par exemple si quelqu'un appuie accidentellement sur le bouton d'extinction de secours de l'onduleur du réseau électrique. Ce type d'erreur provoque d'ailleurs généralement un effet d'entraînement, c'est-à-dire une cascade d'autres problèmes : désactivation du réseau téléphonique, disparition de tous les services de réseau et chaos total. Ce type d'incident est relativement rare ; il représente plutôt l'exception qui confirme la règle.

Comme les infrastructures de réseau tendent à devenir aussi importantes que le réseau téléphonique classique, certaines personnes semblent céder à la paranoïa et craindre de "mettre tous leurs oeufs dans

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

le même panier". Beaucoup de serveurs sont aujourd'hui équipés de plusieurs alimentations. Cela leur permet de rester sous tension si l'une d'elles tombe en panne. Les serveurs sont, en outre, généralement équipés d'un onduleur. Il est d'ailleurs conseillé de brancher chaque alimentation sur un onduleur distinct, sinon, en cas de panne, le serveur s'éteint. Cette approche peut se révéler coûteuse, mais tel est le prix de la sécurité. C'est aux dirigeants de votre entreprise qu'il appartient de décider s'ils sont prêts à déployer les moyens propres à assurer la fiabilité et la tolérance aux pannes.

Vous savez maintenant précisément quel groupe fonctionnel n'est pas opérationnel. Il est temps de sortir de leur tiroir les plans que vous avez tracés avec tant de soin après avoir lu le Chapitre 2. Les utilisateurs du réseau peuvent se plaindre d'une impossibilité à se connecter au serveur, de la disparition des lettres de lecteurs, ou même du plantage de tous les PC de leur secteur. Vous devez alors déterminer si seules les personnes qui viennent se plaindre sont affectées par le problème, ou si tout le monde est concerné. Vous devez également déterminer de quel service de l'entreprise ces personnes font partie. Prenez alors le temps de réfléchir. Si tous les PC parvenaient à se connecter au serveur quelques jours auparavant et si certains n'y parviennent plus maintenant, c'est qu'ils sont défectueux. Le problème peut provenir du câblage Ethernet, d'un commutateur ou d'un serveur:

Examinez les plans du réseau et localisez les personnes concernées. La cause du problème devrait rapidement devenir évidente. A titre d'exemple, si deux services de l'entreprise se plaignent de ne pas pouvoir accéder au réseau, c'est peut-être parce que le' serveur par lequel ils passent est hors-service. Dans ce cas, consultez votre documentation détaillée. De la même manière, si vous constatez, en examinant votre plan fonctionnel, que tous les groupes qui transitent par un routeur donné sont privés de réseau, il est temps de vérifier ce routeur. Si les utilisateurs qui appellent à l'aide sont tous issus d'un même segment de réseau, le problème est vraisemblablement limité à ce segment.Les segments de réseau physiques (qui sont en fait constitués d'une série de concentrateurs) sont particulièrement adaptés à la technique de dépannage consistant à diviser pour régner. Pourquoi un segment de réseau physique tombe-t-il en panne ? Généralement, comme les réseaux utilisent des segments partagés (qui sont en quelque sorte la ligne de distribution commune du réseau téléphonique classique), le problème vient de ce que quelqu'un communique en permanence et empêche les autres de communiquer à leur tour. (Pour plus d'informations, reportez-vous aux chapitres consacrés aux réseaux Ethernet et Token-Ring.) Les mécanismes subtils qu'utilisent les concentrateurs "intelligents" actuels permettent de détecter ce type de problème et d'y remédier. Les problèmes de ce genre sont donc plus rares aujourd'hui.

INFO
Il peut arriver qu'une seule station de travail provoque la panne d'un segment de réseau entier si le réseau n'utilise pas partout des commutateurs. En effet, les concentrateurs intelligents ne sont ni aussi intelligents que vous, ni même aussi intelligents que les fabricants voudraient le faire croire. En d'autres termes, une station de travail donnée peut s'y prendre de différentes manières pour rendre son segment de réseau totalement inexploitable.

Analyse d'un segment défectueux
Comme vous avez pris l'habitude de traiter un système complexe comme un ensemble de systèmes moins complexes (sans chercher à connaître les détails de chacun de ces sous-systèmes), vous n'avez pas réellement besoin de savoir pourquoi le segment est en panne. La seule chose qui vous intéresse, c'est que ce segment est effectivement en panne. La première chose à effectuer pour vérifier qu'un segment est en panne consiste à consulter la documentation physique du réseau pour dénombrer les concentrateurs et les boîtiers de câblage qui font partie de ce segment. Ils sont, en effet, les composants fondamentaux d'un segment physique. Comme un réseau compte généralement beaucoup moins de concentrateurs et de boîtiers de câblage que de PC, il est préférable de commencer par eux. Si votre réseau ne comporte qu'un petit nombre de concentrateurs, vous pouvez parfaitement les isoler un par un pour déterminer à partir de quel moment le problème disparaît. (Dès que le problème disparaît, vous savez que c'est le concentrateur que vous venez d'isoler du réseau qui est en cause.)

Si votre réseau comporte un très grand nombre de concentrateurs, vous devez recourir à la méthode consistant à diviser pour régner. De fait, cette méthode est la plus rapide. Désolidarisez une moitié des concentrateurs du réseau, et déterminez si une station de travail connectée aux concentrateurs restants

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

parvient à se connecter. Si tel est le cas, vous avez loc alisé le segment qui est à l'origine du problème. Sinon, faites un nouvel essai sur l'autre moitié des concentrateurs. Continuez à divi ser en deux, de nouveau en deux, etc., le segment qui pose problème. Vous devriez pouvoir identifier rapidement le concentrateur à l'origine du problème. A ce stade, vous pouvez diviser le concentrateur lui même afin de régner en maître absolu. Testez tous les ports jusqu'à ce que vous trouviez celui qui pose problème (voir Figure 4.2).

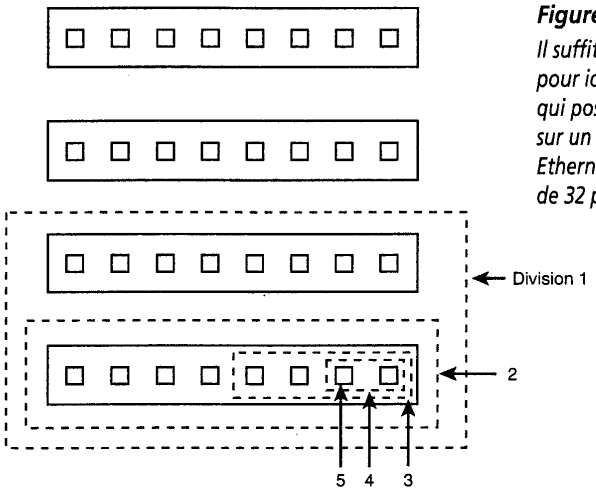


Figure 4.2
Il suffit de cinq essais pour identifier le port qui pose problème sur un concentrateur Ethernet équipé de 32 ports.

Cinq divisions pour localiser un port défectueux sur un concentrateur à 32 ports

INFO

Contrairement à ce qui se passe sur un réseau Token-Ring (sur lequel tous les concentrateurs sont connectés en cercle, comme sur la Figure 4.3), sur un réseau Ethernet, chaque concentrateur est connecté à un autre, en ligne droite (voir Figure 4.5). Cela signifie que si vous désolidarisez un concentrateur du réseau, vous désolidarisez également ceux qui sont placés sous lui. Vous pouvez vous affranchir de cet inconvénient en sautant le concentrateur que vous souhaitez désolidariser du réseau et en connectant directement les câbles que vous venez de débrancher sur le concentrateur suivant de la chaîne. Toutefois, vérifiez que le concentrateur que vous vous apprêtez à configurer en cascade est étiqueté correctement avant d'effectuer la moindre opération. Sinon, vous risquez de ne plus savoir comment les branchements étaient effectués à l'origine.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

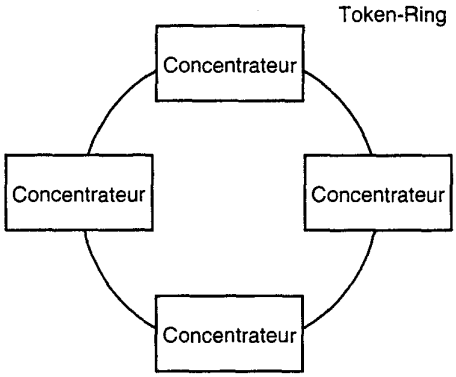


Figure 4.3
Un réseau Token-Ring.

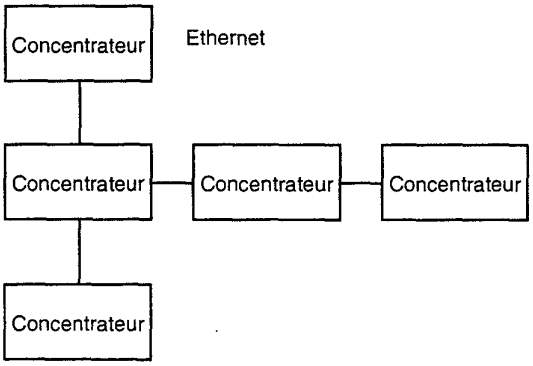


Figure 4.4
Un réseau Ethernet.

Une fois que vous avez localisé le port défaillant - et cela même si vous découvrez du premier coup le concentrateur qui présente un problème de port - effectuez un contrôle de sécurité avant de consi dérer que le réseau est dépanné : remettez le concentrateur en service sur le réseau principal et vérifiez qu'il provoque toujours le problème initial.

ATTENTION
Si vous désolidarisez du réseau le concentrateur principal du réseau, c'est -à-dire celui qui est connecté au serveur ou au routeur qui conduit au serveur - les autres concentrateurs ne seront plus en mesure de "voir" le réseau et ils ne réagiront plus. Si vo us soupçonnez ce concentrateur d'être à l'origine du problème, la meilleure solution est de diviser pour régner au niveau des ports, plutôt que d'isoler complètement le concentrateur du réseau. (Vous devez bien entendu vérifier au préalable que le serveur ou le routeur fonctionnent correctement.) Si vous ne procédez pas de la sorte, vous empêche - rez le serveur ou le routeur de communiquer avec les autres stations de travail du réseau. Vous risquez donc d'en conclure que le concentrateur n'est pas à l'origi ne du problème puisque le réseau ne fonctionne toujours pas quand le routeur est isolé du réseau (car les stations de travail seront toujours incapables d'accéder au serveur ou au routeur). En fait, le problème peut provenir de l'une des stations connectées au concentrateur du serveur. Vous pourrez le détecter en déconnectant les stations de travail, une à une, du concentrateur, au lieu d'ôter l'ensemble du concentrateur.

Si vous devez absolument ôter le concentrateur auquel le serveur ou le routeur sont connectés, vérifiez s'il est allumé ou éteint en consultant votre documentation. Vérifiez également s'il y a des stations de travail actives connectées à ce concentrateur.

Une fois que vous avez identifié le port défectueux, référez -vous à la documentatio n physique de votre réseau et déterminez à quel noeud de réseau il se rapporte. Localisez en dernier lieu le problème local. Le plus souvent, ce type de problème est provoqué par une détérioration d'un câble, par une défaillance d'une carte réseau ou encor e par le plantage d'un PC.

Une fois encore, les concentrateurs "intelligents" sont capables de détecter et corriger automatiquement certains problèmes. Cette straté gie peut donc sembler préhistorique à l'ère de la mise

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

en réseau partagée à transmission automatisée. Toutefois, il est toujours intéressant de savoir comment mener à bien une transmission standard (au cas où vous auriez besoin d'intervenir manuellement) ; de plus, si vous savezdépanner un concentrateur "standard", vous saurez d'autant mieux comprendre le fonctionnement d'un modèle "automatique".

Division du travail

A propos de préhistoire, revenons quelques instants à l'époque des vieux PC fonctionnant sous DOS. Si vous avez déjà travaillé sous DOS, vous savez que sous ce système d'exploitation, quantité de petits programmes, appelés "programmes TSR" (Terminate and Stay Resident, programme résident mémoire) se logeaient dans la mémoire vive de l'ordinateur et empêchaient parfois d'autres programmes de fonctionner correctement. Il se passait la même chose sur les Macintosh d'Apple, à cela près que les programmes TSR étaient appelés "CDEV" ou "INIT". Or, tous ces programmes ne fonctionnaient pas forcément en bonne intelligence les uns avec les autres. A cette époque, si le dépanneur ne disposait pas d'un autre PC ou d'un autre Macintosh, il devait commencer à supprimer ces programmes un par un pour savoir si l'ordinateur recommençait enfin à fonctionner correctement.

Bien entendu, la plupart des techniciens expérimentés recommandaient de commencer par débarrasser l'ordinateur de toutes ces fioritures pour le faire démarrer - c'est-à-dire de désactiver tous les programmes de démarrage. Et à quoi revient cette technique ? A diviser pour régner ! Au lieu d'examiner chacun de ces petits programmes, il suffisait de les supprimer tous et de voir si le problème subsistait. C'est cette stratégie que vous avez utilisée pour résoudre le problème de concentrateur précédent - vous avez divisé en deux groupes les concentrateurs existants, et cela autant de fois que nécessaire, pour identifier le port défectueux.

INFO

Voici comment procéder pour faire démarrer un ordinateur "sans fioritures" sous Windows 95

- Faites démarrer l'ordinateur en mode sans échec en appuyant sur la touche F8 juste après avoir mis l'ordinateur sous tension (mais avant de voir le ciel bleu de l'écran de démarrage de Windows). Vous pouvez ensuite choisir entre Mode sans échec et mode sans échec avec assistance réseau.
- Appuyez sur la touche Maj et maintenez-la enfoncée une fois que l'ordinateur a démarré (cette technique fonctionne également sous Windows NT).
- Voici maintenant comment procéder pour démarrer "sans fioritures" sous DOS
- Appuyez sur la touche F8 après avoir mis votre ordinateur sous tension. Cette opération vous permettra de sélectionner les programmes TSR et les pilotes qui doivent être chargés.

Faites une copie de sauvegarde de vos fichiers AUTOEXEC.BAT et CONFIG.SYS en les renommant AUTOEXEC. BAK et CONFIG. BAK. Ensuite, supprimez manuellement ces deux fichiers de configuration ainsi que tous les pilotes et les programmes TSR. Puis, vous pouvez renommer les fichiers BAK en fichiers AUTOEXEC.BAT et CONFIG.SYS afin de récupérer vos fichiers de configuration initiaux.

Tous les systèmes en réseau que vous rencontrerez bénéficient de cette technique. Même si vous n'êtes plus en environnement monotâche, isolé de tout réseau, cette technique est parfaitement applicable.

Comme nous l'avons vu dans le chapitre précédent, vous pouvez résoudre de nombreux problèmes de réseau en réfléchissant aux modifications qui ont été apportées récemment au réseau. Toutefois, il n'est pas toujours possible de contrôler toutes les modifications, et certaines sont d'ailleurs tout simplement imperceptibles. C'est, par exemple, le cas quand un navigateur, des modules externes ou des définitions de virus ont été mis à jour. Quand les dernières modifications apportées ne sont pas décelables, revenez aux bases des technologies de réseau.

A titre d'exemple, supposez que tous les membres de votre service commencent à éprouver des difficultés à arrêter leur ordinateur. Les ordinateurs se bloquent au moment où le message "Veuillez patienter pendant l'arrêt de votre ordinateur" apparaît à l'écran. Il semble alors que l'ensemble du

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

service soit concerné. Personne ne se rappelle avoir modifié quelque chose récemment, et personne ne comprend ce qui se passe.

Bien que ce problème ne semble pas lié au réseau, le fait qu'il se soit déclaré, spontanément, sur toute une série d'ordinateurs connectés en réseau semble extrêmement étrange. Le constat qui s'impose est que quelque chose a nécessairement changé. Même si l'ingénierie sociale ne parvient pas à révéler la source du changement, vous pouvez toujours diviser pour régner sur votre réseau.

Comme votre service travaille sous Windows 95, nombre des programmes qui s'exécutent au démarrage figurent dans le dossier Démarrage. Vous pouvez supprimer toutes les entrées de ce dossier et réinitialiser l'ordinateur. Vous parvenez de nouveau à éteindre normalement l'ordinateur. Rétablissez la moitié des programmes du menu Démarrage, puis réinitialisez l'ordinateur. Recommencez jusqu'à ce que vous détectiez la source du problème. En fait, il apparaît que c'est votre programme de notification de courrier électronique qui provoque le problème. Toutefois, vous décidez de faire démarrer l'ordinateur en ne chargeant que le programme de notification de courrier électronique, et cette fois aussi, vous parvenez à éteindre l'ordinateur.

Dans ce cas, vous êtes confronté à un problème d'interaction. Pour le résoudre, vous pouvez continuer à diviser pour régner. Vous rétablissez la moitié des programmes qui figuraient dans le dossier Démarrage et vous constatez que le problème se pose quand le programme de notification de courrier électronique et l'antivirus sont chargés tous les deux. En fait, l'antivirus, qui se met à jour automatiquement à partir de l'Internet, est entré en conflit avec le programme de notification de courrier électronique. Une visite rapide sur le site Web du fabricant du logiciel de courrier électronique (et non de l'antivirus) vous permet de trouver un patch pour le logiciel client de courrier électronique. Voilà votre problème résolu.

Evidemment, la méthode consistant à diviser pour régner ne permet pas de résoudre tous les problèmes. En particulier, il est difficile de dépanner les problèmes intermittents et quantitatifs (plutôt que qualitatifi) qui ne correspondent pas à un cas de figure si radical.

A titre d'exemple, la méthode consistant à diviser pour régner peut vous conduire à la conclusion que c'est une nouvelle application que vous venez d'installer qui ralentit votre réseau (et vous avez peut-être raison). Toutefois, il n'est pas toujours possible de se séparer d'une nouvelle application, installée parce que les utilisateurs en avaient besoin. De surcroît, il n'est pas certain que ce soit l'application qui soit en cause. Le réseau peut, en fait, souffrir d'une saturation générale. Dans ce cas, vous pouvez essayer de remplacer l'application par une autre. Mais êtes-vous réellement en mesure de désinstaller, en très peu de temps, une application déjà largement déployée sur le réseau ? Dans la pratique, vous finirez probablement par vérifier que l'application est bien configurée et par faire en sorte qu'elle fonctionne correctement sur le réseau.

Conclusion : même si la méthode consistant à diviser pour régner ne vous permet pas de résoudre systématiquement votre problème, elle peut au moins vous aiguiller dans la bonne direction.

XI-3- LE JEU DE L'INTRUS

Comme son nom l'indique, la technique de dépannage du "jeu de l'intrus" est beaucoup plus un jeu qu'un travail lourd et pénible. File constitue l'un des moyens les plus gratifiants et les plus amusants de dépanner un réseau. Le principe est le suivant : dès lors qu'un réseau est composé d'au moins deux éléments identiques, si l'un d'eux ne fonctionne pas correctement, il suffit de le comparer à un autre qui fonctionne pour trouver la cause du problème.

Dans la pratique, en effet, quand deux éléments, censés être identiques, présentent des différences, ce sont généralement ces différences qui provoquent des dysfonctionnements.
Il en va de même quand un périphérique ne fonctionne pas sur un réseau : si vous parvenez à trouver un périphérique identique qui fonctionne parfaitement, il suffit probablement de calquer la configuration de celui qui ne fonctionne pas sur celle du périphérique qui fonctionne pour résoudre le problème.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Serveurs et routeurs

Cette règle est applicable à tous les composants d'un réseau, mais elle présente des limites dans le domaine du dépannage des serveurs et des routeurs. Un routeur ou un serveur donnés sont rarement rigoureusement identiques à un autre routeur ou serveur, bien qu'ils puissent jouer un rôle similaire. Parfois, la similitude du rôle joué par deux systèmes est suffisante pour dire que ces deux systèmes sont comparables.

Les serveurs et les routeurs présentent des similitudes au niveau de leur intégrité. Ainsi, quand un routeur se bloque systématiquement alors que tous les autres fonctionnent parfaitement, c'est souvent parce qu'il utilise un système d'exploitation (ou microcode) d'une autre version. Les routeurs matériels ne fonctionnent pas sous Windows ou sous DOS. Ils utilisent un système d'exploitation très simple (contrairement à Windows, qui utilise une multitude de fichiers . DLL). Il suffit donc généralement de contrôler le numéro de révision du routeur défectueux pour constater qu'il diffère de celui des routeurs qui fonctionnent correctement.

De la même manière, il est très facile de comparer les patchs et les fichiers . DLL installés sur un serveur Windows NT instable, à ceux d'un serveur Windows NT qui fonctionne parfaitement. Les serveurs NetWare, notamment, possèdent un utilitaire appelé Config Reader (voir Chapitre 13), qui compare avec une efficacité étonnante les dizai
nes de modules NLMS (NetWare Loadable Modules, modules chargea
bles par NetWare) et les patchs qui sont installés sur un serveur.

Objets utilisateur

Comme les serveurs sont tous configurés légèrement différemment les uns des autres, il est préférable d'appliquer le principe du jeu de l'intrus aux objets utilisateur existant sur votre réseau. Par convention, les objets utilisateur (les noms d'utilisateurs, les mots de passe, les droits d'accès et les stations de travail elles-mêmes) sont toujours configurés d'une manière similaire - ne serait-ce que parce que votre consultant en réseaux a probablement trouvé plus facile de s'appuyer systématiquement sur le même modèle de référence pour configurer le réseau.

Sous sa forme la plus simple, le jeu de l'intrus est relativement facile. Supposons qu'un groupe d'utilisateurs travaille dans de bonnes conditions depuis un certain temps. Soudain, l'un d'eux vient se plaindre qu'il ne parvient pas à utiliser une application donnée. Puisque les. autres utilisateurs travaillent avec leur propre nom d'utilisateur et sur leur propre station de travail, la première chose à faire est de déterminer si le problème ne vient pas du nom d'utilisateur ou de la station de travail de l'utilisateur privé de l'application en question. En procédant par élimination, vous pouvez mettre hors de cause la station de travail en demandant à l'utilisateur d'ouvrir une session sur une autre station de travail. S'il ne parvient toujours pas à ouvrir l'application, vous pouvez en déduire que c'est son nom d'utilisateur (et non la station de travail) qui pose problème. Vous pouvez d'ailleurs vous livrer à une expérience supplémentaire pour vous en assurer : demandez tout simplement à une autre personne d'aller ouvrir une session sur la station de travail que vous souhaitez mettre hors de cause. Si cette personne parvient à ouvrir l'application concernée, c'est bel et bien du nom d'utilisateur que vient le problème. Il ne vous reste plus ensuite qu'à déterminer dans quelle mesure le nom d'utilisateur de la personne qui ne peut pas charger l'application diffère de celui des utilisateurs qui le peuvent.

ATTENTION

Ne comparez que des choses comparables. En d'autres termes, si vous essayez de charger une application sur une station de travail sur laquelle l'application n'a pas été installée, vous rencontrerez forcément des problèmes. Par ailleurs, certaines applications enregistrent des fichiers spécifiques à l'utilisateur sur le disque dur de la station de travail, et non sur celui du serveur. Méfiez-vous, par conséquent, de ces applications. Effectuez un contrôle expérimental pour chaque type d'application -avant même d'être confronté à des problèmes - pour savoir si un utilisateur qui peut travailler sous une application donnée sur son PC peut également la charger sur un autre PC. Si tel est le cas, vous saurez que l'application est capable de "flotter" d'une station de travail à une autre.

INFO

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Quand seul un petit nombre d'utilisateurs d'un groupe de travail donné déplore un problème, intéressez-vous d'abord aux éléments qui ont changé. Si vos recherches restent vaines ou, pire encore, si la seule modification que vous avez effectuée est impérative pour le bon fonctionnement du rés eau, intéressez-vous aux différences qui distinguent ces utilisateurs du reste du groupe de travail.

INFO

La technique de l'élimination est particulièrement efficace quand deux objets présen tent plusieurs différences. A titre d'exemple, si deux stations de travail sont équipées de cartes vidéo, de cartes réseau et de quantités de RAM différentes, vous pouvez commencer par les équiper de la même quantité de RAM. Ensuite, vous pouvez y instal ler deux cartes réseau identiques, etc.implicité, le maître-mot du dépannage réussi

A ce stade de cet ouvrage, vous avez probablement compris qu'il est essentiel de rester simple pour être un dépanneur efficace. C'est d'ailleurs précisément ce que vous faites quand vous commencez par examiner l'objet de haut niveau pour déterminer quel élément n'est pas identique aux autres (voir figure 5.1). Dans l'exemple précédent, pourquoi examiner la configuration de la station de travail alors que vous disposez d'un moyen de vérifier qu'elle n'est pas en cause ? De même, pourquoi remplacer la carte vidéo ou la carte réseau alors que vous savez pertinemment que l'ordinateur n'est pas à l'origine du problème ?

Il est très pratique de se représenter ces éléments comme s'ils étaient enfermés dans des conteneurs de haut niveau, renfermant eux-mêmes des conteneurs de niveau inférieur. Tant que vous ne pouvez pas mettre hors de cause (ou en cause) un conteneur de haut niveau, il ne sert à rien de vous intéresser à ses sous-conteneurs. Il est possible de se repré senter une configuration de réseau type ccmme une "boîte de stations de travail" (qui contient des cartes mères, de la mémoire, des disques durs, etc.), une "boîte de matériel de réseau" (qui contient des câbles, des concentrateurs, des commutateurs, etc.) et une "boîte d'utilisa teurs" (qui contient des noms d'utilisateurs, des scripts d'ouverture de session, différents attributs de sécurité, etc.)

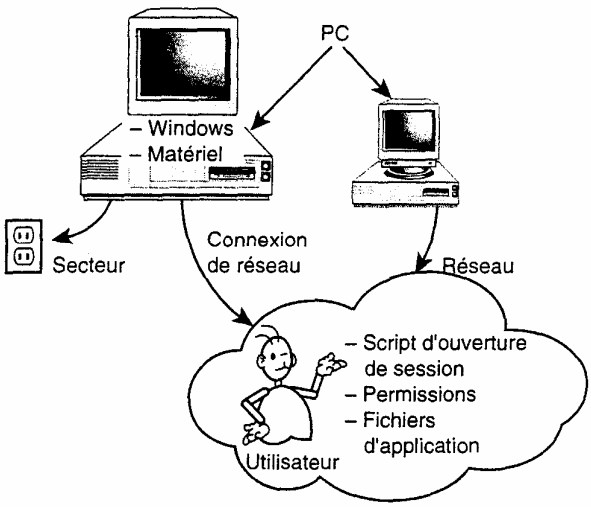


Figure 5.1
Commencez toujours par examiner les objets de haut niveau.

Grâce à cette représentation sous forme de boîtes, vous pouvez vous concentrer sur le problème auquel vous êtes confronté sans être distrait par autre chose. Si vous découvrez que c'est du réseau que vient le problème, vous ne serez pas tenté de vous intéresser aux sous-composants des stations de travail, par exemple. En d'autres termes, une fois que vous avez établi que c'est le réseau qui pose problème, vous ne devez plus vous intéresser qu'aux sous-composants de ce réseau..

Régulariser de force ou non ?

Une fois que vous avez cerné la zone du problème, la solution la plus rapide consiste à régulariser de force la situation des éléments qui ne sont pas identiques aux autres - afin de rendre un élément qui pose problème identique à celui qui fonctionne parfaitement.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Toutefois, sur la base de quels critères effectuer cette régularisation ? Pour être efficace, vous devez remplacer sans état d'âme - c'est-à-dire sans perdre de temps à chercher quel élément précis joue les troublefête - tous les éléments qui, à l'intérieur d'un conteneur, ne sont pas identiques à ceux d'un autre conteneur censé être semblable.

La duplication de lecteurs peut constituer une aide précieuse à ce niveau. En effet, il est facile de régulariser la configuration d'un disque dur qui fonctionne mal en prenant modèle sur un autre qui fonctionne parfaitement. Dans le domaine de la "régularisation de force", vous pou vez également avoir intérêt à - recréer le répertoire principal de l'utilisateur, et ceci une fois que vous avez cerné la zone principale du problème. A titre d'exemple, les programmes UNIX sont dépendants de plusieurs fichiers de configuration stockés dans le répertoire principal d'un utilisateur. Vous pouvez alors renommer ce répertoire principal, en créer un nouveau pour l'utilisateur concerné, puis y copier le contenu d'un autre répertoire principal (appartenant à un autre utilisa teur) qui fonctionne correctement. (voir figure 5.2).

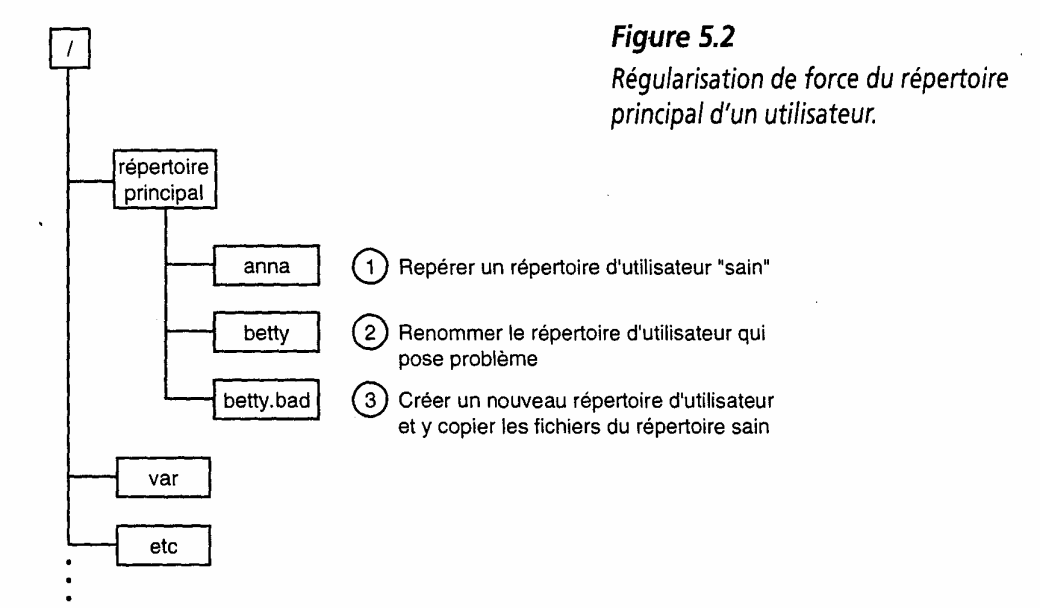


Figure 5.2
Régularisation de force du répertoire principal d'un utilisateur.

Si vous ne pouvez pas utiliser cette technique (parce que vous ne pouvez pas écraser des informations cruciales pour le réseau, par exemple), examinez les éléments suivants, présentés par ordre de priorité décroissant de gauche à droite

- Station de travail
- BIOS/fabricant
- Disque dur

Configuration du système d'exploitation (fichiers de démarrage, registre)

Composants du système d'exploitation (fichiers DLL)

- Applications locales
- Virus ? Ou non ! - Carte réseau
- Câble
- Carte vidéo - RAM
- Alimentation
- Onduleur
- Parasurtenseur

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

- Nom d'utilisateur sur le serveur
- Script d'ouverture de session - Permissions
- Fichiers de configuration des applications (liste d'accès

orientée utilisateur ?)

- Fichiers d'utilisateurs (répertoire principal)
- Application elle-même
- Port du commutateur ou du concentrateur

INFO

Nombre de gens n'ont pas pleinement conscience des conséquences désastreuses que peut générer un secteur électrique (courant de 220 V AC) instable. Or, il est très utile de pouvoir mettre hors de cause le secteur quand un PC plante au moment de se connecter au réseau. Pour cela, il suffit dé brancher le PC sur une autre prise de courant ou d'ajouter un filtre de courant électrique. Un filtre de courant électri que est un système qui permet de débarrasser le courant de ses fluctuations et de ses absences (notamment dans les zones rurales).

Une fois encore, fuyez les composants de bas niveau. A titre d'exemple, le système d'exploitation peut valoir à lui seul une semaine de recherches et d'essais infructueux., Vous pouvez passer des journées entières à comparer tous ces objets de bas niveau. Le jeu peut en valoir la chandelle dans certains cas. Cependant, quand le problème n'affecte qu'une zone limitée, les informations dont vous n'avez pas besoin sont des informations indésirables. On peut parler de masquage délibéré d'informations. Ayez toujours à l'esprit l'exemple de la pompe à essence du début de ce livre, surtout quand vous devez vous plonger dans des zones plus détaillées que ce que vos compétences vous permettent réellement d'appréhender. Avez-vous vraiment besoin de connaître toutes les subtilités des différents fichiers . DLL de Windows, alors que vous pouvez vous contenter de les copier à partir d'un autre ordinateur qui fonctionne correctement ?

A l'inverse, si votre logiciel de courrier électronique génère un message d'erreur indiquant, par exemple, qu'il ne peut pas charger le fichier MAPI32. DLL, il est toujours intéressant de rechercher ce fichier sur le disque dur de l'ordinateur et de l'examiner de plus près. Il se peut que le fichier existe, mais qu'il soit endommagé (il peut afficher une taille de 0 Ko, par exemple). Vous pouvez aussi le comparer au fichier MAPI32. DLL d'un autre ordinateur qui fonctionne correctement, et constater que le fichier MAPI32. DLL signalé absent est beaucoup plus petit que celui de l'ordinateur qui fonctionne. Dans ce cas, le plus simple est de copier ce fichier à partir de l'ordinateur qui fonctionne, plutôt que de réinstaller et de reconfigurer l'ensemble de la station de travail. C'est à vous qu'il incombe de prendre la bonne décision au bon moment. Suivant la situation dans laquelle vous vous trouvez, examinez les informations dont vous disposez, demandez-vous combien de temps prendront les différentes solutions qui s'offrent à vous et choisissez celle qui semble la plus rapide et la plus efficace.

Voici maintenant l'aspect le plus délicat de la méthode du jeu de l'intrus : trouver quels éléments comparer et mettre le doigt sur. celui qui pose problème. A titre d'exemple, si plusieurs utilisateurs (mais pas tous) se plaignent d'un problème, surtout s'il est intermittent, il peut être difficile de savoir par où commencer. Dans pareil cas, commencez par consigner dans un journal tous les appels à l'aide que vous recevez. Recensez ensuite dans un tableau tous les problèmes qui se posent, le moment où ils sont apparus ainsi que la configuration des stations de travail et le nom des utilisateurs concernés. Voir tableau 5.1.

Si vous examinez attentivement ce journal détaillé, vous pourrez constater que les erreurs les plus fréquentes sont des erreurs de fonctionnement illégal. (Si cette liste recensait davantage d'incidents, cela serait plus évident encore. Les autres entrées de ce journal ne sont que des nids de poule qui jalonnent la route, et non des erreurs graves.) A ce stade, vous savez donc que "certains de, ces éléments ne sont pas identiques aux autres". Ceux qui sont identiques entre eux sont les erreurs récurrentes, que vous devez maintenant vous attacher à résoudre.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Tableau 5.1 : Exemple de journal d'incidents

Date	Heure	Service	Utilisateur	Problème	Type de PC
11/8	2 H 00	Comptabilité	Jacques	Erreur de fonctionnement illégal — Word Perfect	Clone/486
11/8	2 H 20	Comptabilité	Annie	Exception fatale 06 (pendant le démarrage de l'ordinateur). Tout a semblé OK ensuite.	Dell/P6
11/8	3 H 00	Comptabilité	Elodie	Erreur de fonctionnement illégal Word Perfect	Clone/486
12/8	9 H 00	Comptabilité	Elodie	Erreur de fonctionnement illégal Word Perfect	Clone/486
12/8	10 H 45	Comptabilité	Jacques	Erreur de fonctionnement illégal Word Perfect	Clone/486
12/8	13 H 00	Comptabilité	Gilles	Plantage. A dû réinitialiser l'ordinateur pendant qu'il lisait son courrier électronique.	Clone/486
13/8	11 H 00	Comptabilité	Jacques	Erreur de fonctionnement illégal Word Perfect	Clone/486
12/8	12 H 45	Comptabilité	Bertrand	Erreur de fonctionnement illégal Word Perfect	Clone/486

Pourquoi Bertrand n'appelle-t-il pas aussi souvent qu'Elodie ? Un coup de fil rapide vous permet de savoir qu'il était en rendez-vous à l'extérieur les 11 et 12 août, et qu'il aurait sans doute appelé plus souvent s'il avait été là.

Prenons maintenant un exemple concret. Vous avez la charge de mettre à niveau un réseau et de le faire migrer vers Windows 95. Vous devez également le faire migrer vers une nouvelle version de Word Perfect. Votre chef de service vous a signalé qu'il s'agissait là d'une migration stratégique, ce qui signifie en substance qu'en cas de dysfonctionnement il n'est pas possible de remettre le réseau dans son état d'origine. Vous êtes donc tenu à une obligation de résultat. Alors que les ordinateurs pilotes que vous avez utilisés pour vos tests fonctionnaient parfaitement, un jour ou deux après la mise à jour, vous commencez à rencontrer des problèmes. Certains utilisateurs (mais pas tous) signalent des erreurs de fonctionnement illégal. Or, vous êtes absolument certain que tous les utilisateurs ont été configurés de la même manière, avec les mêmes scripts d'ouverture de session, les mêmes permissions d'accès et la même configuration de répertoire principal. Malheureusement, comme vous avez dû utiliser des PC clonés, vous n'êtes pas aussi certain que toutes les stations de travail soient identiques.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Vous consignez les incidents pendant plusieurs jours dans votre journal, et vous découvrez que certains utilisateurs ne signalent jamais cette erreur. Vous en concluez donc que le problème n'est pas itinérant. Il se produit toujours aux mêmes endroits. Il s'agit là d'une avancée non négligeable. En effet, certaines erreurs n'apparaissent pas toutes au même endroit ni au même moment ; elles se déplacent de station de travail en station de travail, ce qui indique que le problème est systémique, et non limité à des stations de travail précises.

Ensuite, vous constatez que seuls les ordinateurs clonés sont affectés par le problème d'erreur de fonctionnement illégal. Aucun des utilisateurs d'ordinateurs de marque n'a signalé quoi que ce soit à ce niveau. Enfin, vous remarquez que tous les utilisateurs d'ordinateurs clonés ne vous ont pas signalé cette erreur. Seuls certains sont concernés. Vous en venez donc à penser que certains de ces ordinateurs contiennent des composants défectueux.

De toute évidence, parmi ces ordinateurs clonés, certains ne sont pas identiques aux autres ! Afin de mettre les utilisateurs hors de cause, interchangez un ordinateur dont le propriétaire vous a appelé pour vous signaler le problème avec un autre ordinateur dont le propriétaire n'a rien signalé. Comme l'utilisateur qui n'avait rien signalé se plaint maintenant du même problème, vous avez la certitude que la station de travail est en cause.

Procédez à un inventaire des stations de travail affectées par le problème afin de chercher ce qu'elles ' ont en commun. Créez un nouveau tableau dans lequel vous recensez les objets de bas niveau (voir Table au 5.2). Prenez le parti de mettre hors de cause Windows 95 et ses composants, car vous avez tout mis en oeuvre, pendant la mise à jour du réseau, pour configurer toutes les stations de travail rigoureusement de la même manière. Ne prenez pas non plus la peine de vérifier que le réseau n'est pas infecté par un virus, car vous avez employé un antivirus durant l'installation de Windows 95.

Tableau 5.2 : Exemple de tableau de composants de bas niveau

Station de travail	BIOS	Carte vidéo	Disque dur	RAM	Concentrateur /port
Jacques	AMI	Marque X	Quantum	16 Mo	8/2
Elodie	Phoenix	Marque X	Conner	16 Mo	9/3
Bertrand	AMI	Marque X	Seagate	24 Mo	8/1

A la lecture de ce tableau, il apparaît que tous les ordinateurs sont équipés d'un matériel tout à fait actuel. Cependant, cet inventaire montre que l'assembleur des PC a pris "ce qu'il avait sous la main" pour les monter. Toutefois, bizarrement, il apparaît que tous les PC clonés sont équipés de la même carte vidéo.

Comme l'opération est très simple, vous interchangez la carte vidéo de l'une des stations de travail défectueuses avec celle d'une autre station de travail "saine". Vous constatez alors que la station de travail n'est plus défectueuse. Vous interchangez une nouvelle fois la carte que vous venez d'installer avec une autre appartenant à une station de travail "saine" : là encore, le problème ne se manifeste plus. Vous essayez alors de mettre à jour les pilotes de la carte vidéo des stations de travail défectueuses, mais rien n'y fait. La seule solution possible consiste à remplacer toutes les cartes vidéo, ce que vous faites : toutes les stations de travail défectueuses se mettent alors à fonctionner normalement.

Bien entendu, plus les composants des stations de travail d'un réseau différent d'une station à l 'autre, plus le dépannage est délicat. Moins il y a de différences entre les stations de travail, moins il faut de temps pour déterminer l'élément dissemblable. Mieux vaut donc effectuer un dépannage préventif en essayant de toujours vous conformer aux mêmes standards en termes de logiciels, de matériel, etc., surtout au sein d'un même service ou groupe de travail.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

INFO
Un réseau hétérogène est un réseau dont tous les composants sont différents. Dans pareil cas, il est évidemment très difficile d'utiliser le principe du jeu de l'intrus pour résoudre les problèmes. Un réseau homogène, à l'inverse, est un réseau dont tous les composants sont quasiment identiques. Il s'agit là de l'environnement de travail idéal pour l'adepte du jeu de l'intrus.

Mais existe-t-il vraiment des réseaux parfaitement homogènes, dont tous les composants sont parfaitement identiques ? Probablement pas. Néanmoins, la règle d'or est que les différents composants d'un réseau doivent toujours comporter autant de caractéristiques identiq ues que possible.

XI-4- DONNEES SUBJECTIVES, DONNEES OBJECTIVES, ANALYSE ET PLAN: LES QUATRE INSEPARABLES

Vous avez été intéressé par le Chapitre 5 ? Tant mieux, car la méthode de dépannage que vous allez découvrir dans le présent chapitre s'inscrit dans le prolongement direct de la précédente. Pour traiter un problème complexe, il faut généralement prendre beaucoup de notes ; cela permet ensuite d'éclaircir les zones de flou qui entourent le problème. Jusqu'ici, vous avez traité les problèmes de la même manière que pour remplir un questionnaire à choix multiples - en analysant les change-inents, en raisonnant par divisions et en cherchant les différences. La tâche est maintenant un peu plus complexe, puisque vous êtes face à un questionnaire à trous. Vous allez devoir patauger dans le subjectif, le faire correspondre à l'objectif, analyser vos données et établir un plan pour déterminer la conduite à tenir. En d'autres termes, vous allez enfin vous attaquer à des problèmes vraiment ardus.

Docteur réseau
Le métier de dépanneur de réseaux s'apparente à celui de médecin. Mais, d'une certaine manière, la médecine est une activité plus difficile que le dépannage de réseaux. En médecine, il n'existe guère de stan - dards. Les géniteurs ne diffusent jamais de fiches techniques sur le produit de, leurs entrailles (et encore moins une documentation complète) et le sujet sur lequel vous opérez peut vous poursuivre en justice en cas d'erreur. Les médecins recourent à quantité d'astuces de diagnostic, qui peuvent également être très utiles à un dépanneur de réseaux.
Parmi ces astuces figure la méthode des quatre inséparables. Sur la fiche de consultation de leurs patients, certains médecins réalisent quatre colonnes intitulées respectivement "Données subjectives", "Données objectives", "Analyse" et "Plan". Quand un patient consulte un méde cin parce qu'il a mal à l'estomac, le praticien peut écrire

- Données subjectives. Le patient se plaint d'avoir mal à l'estomac ; il a mangé des cuisses de poulet à la sauce diable la nuit précédente ; il a travaillé très tard.
- Données objectives. Une palpation de l'estomac révèle que le quart supérieur droit est anormalement mou.
- Analyse. Risque de gastrite aiguë.
- Plan. Traitement à l'antiacide pendant 5 jours ; léger régime ; nouvelle cons ultation dans 5 jours pour un nouveau diagnostic.

Les données subjectives correspondent à ce que dit le patient au médecin. Les données objectives correspondent à ce que le médecin constate. L'analyse est ce que le médecin déduit à partir de ses questions supplémentaires et de son raisonnement. Le plan est ce qu'il envisage de faire pour traiter le problème. Cependant, les médecins sont habitués à rece voir des réponses imprécises des patients. Toutefois, s'ils disposent d'un plan, ils sont à peu près cer tains d'aller dans la bonne direction.

La méthode des quatre inséparables permet d'aller dans la bonne direc tion. En tant que dépanneur de réseaux, vous n'aurez pas toujours la chance de pouvoir résoudre tous les problèmes en un jour ou une semaine. Certains d'entre eux ne sont qu'intermittents, et ils nécessi tent généralement une stratégie très complexe, s'inscrivant sur le long terme. Pour parvenir à cerner un problème complexe, vous devez abso - lument en discerner les composantes : l'événement tel qu'i l est signalé de manière subjective pàr les utilisateurs d'une part, et les faits objectifs d'autre part. Il est particulièrement important de faire abstraction

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

de l'aspect subjectif - un utilisateur peut vous signaler quelque chose effectivement lié au problème, mais il n'est pas certain que ces informations vous aiguillent dans la bonne direction. Imaginez un malade qui signale une douleur poitrinaire. Faut-il en déduire qu'il est victime d'une attaque cardiaque ou simplement qu'il souffre d'un problème musculaire ? Le mal dont se plaint le patient est une sensation subjective ; l'investigation active qui révèle une attaque cardiaque ou un problème musculaire est la découverte objective. Les données subjectives sont certes utiles, mais elles doivent impérativement être assorties d'une investigation.

Des faits, rien que des faits

Pour résoudre un problème de réseau particulièrement complexe ou intermittent, essayez de réunir un certain nombre d'informations objectives, qui pourront vous orienter vers une solution viable :'

- durée du problème (problème permanent ou intermittent ?) ;
- date et heure auxquelles le problème a commencé à se manifester ;
- endroit concerné (emplacement physique sur le réseau) ;
- nombre d'utilisateurs concernés ;
- configuration de la station de travail (identique aux autres ou différente ?) ;
- nombre et type des applications concernées (avec quelles autres applications fonctionnent-elles ?) ;
- nom des utilisateurs concernés, ainsi que des groupes de sécurité dont ils font partie ;
- mesures ;
- comportement des applications similaires.

Même si vous disposez d'un grand nombre de données objectives, vous ne possédez pas nécessairement l'information objective pour aboutir à la bonne conclusion. Pour vos premières tentatives de résolution d'un problème particulièrement complexe, votre "plan" consistera donc, probablement, à collecter davantage d'informations. Ne renoncez pas à ce plan ; plus vous disposerez d'informations, plus vos suppositions ont de chances de se vérifier.

Mise en pratique de la méthodedes quatre inséparables

Imaginons un cas où un utilisateur se plaint de ne pouvoir exécuter une applet Web donnée dont il a besoin pour son travail. La Figure 6.1 présente un plan logique du site. Le PC est situé au point A du plan.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

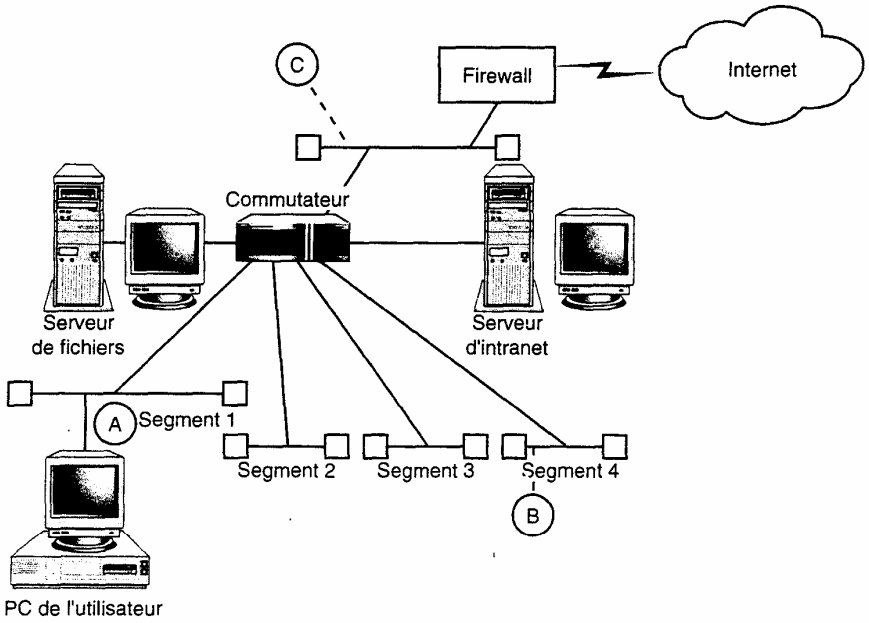


Figure 6.1

Dépannage d'un problème lié à une plage horaire.

Vous allez voir le PC de l'utilisateur et vous parvenez parfaitement à faire fonctionner l'applet. L'utilisateur essaie de nouveau l'applet, qui s'exécute parfaitement, mais vous signale de nouveau ce problème le lendemain. Vous décidez d,'employer la méthode des quat re inséparables pour trouver une solution

- Données subjectives. L'applet Web ne fonctionne pas.
- Données objectives. L'applet fonctionne parfaitement quand c'est vous qui l'exécutez.
- Analyse. Peut-être l'heure à laquelle l'applet est exécutée entre-t-elle en ligne de compte ?
- Plan. Vous décidez de retourner voir le PC à l'heure à laquelle l'utilisateur essaie généralement d'exécuter l'applet.

Votre analyse du problème est très pertinente, et votre plan consistant à collecter de nouvelles informations fonctionne. Vous allez voir l'utilisateur à l'heure à laquelle il rencontre habituellement le problème et vous essayez d'exécuter son applet Web. Bien entendu, elle ne fonctionne pas. Que se passe-t-il ? Cette fois, c'est vous qui fournissez les informations subjectives - qui sont votre supposition

- Données subjectives. Vous pensez que l'heure à laquelle l'applet est utilisée a un lien avec le dysfonctionnement.
- Données objectives. L'applet refuse de fonctionner à 8 H 00.
- Analyse. Le problème ne serait-il pas dû à une autre activité de réseau qui aurait lieu au même moment sur ce segment ?
- Plan. Vous décidez d'essayer l'applet sur un autre segment de réseau (point B du plan).
- Ce plan est parfaitement sensé, mais il ne fonctionne pas
- Données subjectives. L'activité de réseau peut être différente sur, le segment de l'utilisateur à 8 H 00.
- Données objectives. L'applet refuse toujours de fonctionner sur un autre segment.
- Analyse. Quel autre facteur peut être différent à pareille heure ?
- • Plan. Vous décidez de recenser les événements qui ont lieu sur l'ensemble du réseau à

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

8 H 00.

Le problème continue de se manifester à 8 H 00, même si l'utilisateur change de segment. Parfait ! Son segment de réseau est maintenant hors de cause, ce qui représente une avancée très importante. Vous avez fait une déduction et elle s'est révélée fausse.

Est-ce un virus, docteur ?

Vous vous demandez si le réseau n'est pas contaminé par un virus qui se déclencherait à 8 H 00 un jour précis. Mais vous rejetez bien vite cette hypothèse car v ous disposez d'une protection relativement efficace contre les virus. De plus, quand vous avez testé l'applet Web sur l'autre segment, vous avez utilisé une station de travail saine. Cette supposition était néanmoins très pertinente, car il existe vraiment des virus de ce type - des virus qui ne font absolument pas parler d'eux jusqu'à une certaine date et une certaine heure. A échéance, ils activent leurs effets dévastateurs sur le réseau qu'ils ont infecté.

Vous voilà donc reparti en quête de nouvelles hypothèses.

Le docteur a besoin d'une consultation

Ce moment est très important, car vous êtes vexé et découragé. Vous pensez que vous ne parviendrez jamais à résoudre le problème. Vous avez même envie de tout abandonner. Mais rassurez-vous, même les "pros" sont parfois en proie à des envies de ce type. Or, la force d'un dépanneur digne de ce nom est qu'il sait faire une pause et réexaminer la situation ensuite. Comme un médecin, un dépanneur peut avoir besoin d'une "consultation" auprès d'un confrère pour pouvoir appréhender un problème sous un nouvel angle.

Devez-vous vraiment vous adresser à un dépanneur professionnel pour éclairer votre lanterne ? Pas vraiment. Si vous avez besoin de l'avis d'un tiers, c'est simplement parce que vous êtes trop près du problème et que vous êtes embarrassé par un certain nombre d'idées préconçues. En fait, vous pouvez vous adresser à n'importe qui pour demander ce qui peut bien se passer tous les matins à 8 H 00. On vous répondra probablement que "tous les utilisateurs mettent leur PC sous tension" ou que "tous les employés se mettent au travail". Et soudain, votre lanterne s'éclaire enfin. Comme tous les utilisateurs mettent leur PC sous tension et ouvrent une session à 8 H 00, cette heure pourrait bien correspondre au x heures de pointe du réseau routier que vous emprun - tez tous les jours pour aller au travail.

Comment vous en assurer ? Il existe deux solutions. Vous pouvez :

- effectuer des mesures (ce qui est relativement délicat),
- changer d'endroit (déplacer la statio n de travail à un endroit où le trafic est moins dense).

Certes, vous avez déjà déplacé la station de travail sur un autre segment, mais ce segment peut lui aussi poser problème. C'est un peu comme rouler sur les Champs -Elysées, au lieu de rouler place de la Concorde - cela ne vous avance pas à grand -chose si vous devez abso lument vous déplacer aux heures de pointe. (D'une certaine manière, vous avez considéré qu'il y avait des travaux ou un accident place de la Concorde, mais pas sur les Champs-Elysées.) Maintenant, la méthode des quatre inséparables vous permet de disposer des quatre éléments suivants :

- Données subjectives. Le problème peut être dû à une saturation du réseau.
- Données objectives. Le problème apparaît au même moment sur les différents seg ments de réseau majeurs.
- Analyse. Il est probable que le nombre des ouvertures de session provoque une saturation sur un segment majeur, mais c'est moins vraisemblable sur un segment fréquenté par moins d'utilisateurs.
- Plan. Vous décidez de consulter vos p lans et d'essayer l'applet sur un segment de réseau donnant lieu à un trafic moins dense (à proxi mité du segment reliant l'Internet, par exemple, et à l'écart des segments qui transmettent au serveur des informations sur les

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

ouvertures de session).

Vous déployez votre plan. Vous installez temporairement une station de travail au niveau du point C de la carte. Quand vous essayez l'applet à 8 H 00, elle fonctionne ! Le problème est donc bel et bien dû à une satu ration du réseau. Il vous reste maintenant à déterminer à qui vous adres ser pour résoudre le problème. En d'autres termes, devez-vous vous en prendre au concepteur de l'applet pour ne pas avoir analysé correctement votre réseau, ou à vous-même pour avoir accepté que certains segments de réseau puiss ent être sollicités à ce point ?

La réponse à cette question peut varier. D'un côté, il peut être intéres sant de déplacer l'utilisateur qui se plaint du problème pour l'affecter à un segment de réseau moins sollicité. De l'autre, cette solution n'est pas nécessairement viable, d'autant que vous avez vu, sur le plan physique du réseau, que les segments situés près des PC incluent déjà un grand nombre de PC et sont placés en plein milieu des serveurs. En d'autres termes, des contraintes physiques peuvent vous empêcher de placer cette personne sur un segment dépourvu de PC, car les seuls concentrateurs situés à proximité d'elle sont déjà utilisés par d'autres personnes. Le seul concentrateur soumis à un trafic peu intense est placé en plein milieu de votre c entre de données, ou dans un autre bâtiment, où cette personne n'a pas sa place. (Bien entendu, des petits malins auront toujours l'idée de proposerr que cette personne arrête de travailler à 8 H 00 du matin, mais cette solution est absurde. Le réseau a ét é conçu pour fonctionner!)

A ce stade, si vous avez vraiment besoin de laisser la station de travail de cette personne sur un segment de réseau très actif, vous devez dépanner l'applet elle -même. Vous devez déterminer pourquoi cette personne rencontre des problèmes avec l'applet, mais pas avec les appli cations locales. Il est déconseillé de comparer une application locale à une application Internet (voir Chapitre 16). Les applications Internet sont aux applications locales ce que sont les vols long - courrier aux trajets pour se rendre à l'hypermarché du coin. Il peut se passer quan tité de choses entre votre site et New York, par exemple. Vous reformu lez donc le problème de la manière suivante

- Données subjectives. L'applet ne fonctionne pas ; les autres ap plications, en revanche, sont parfaitement opérationnelles.
- Données objectives. L'applet est la seule application Internet du lot.
- Analyse. Les applications Internet ne sont pas des applications locales.
- Plan. Vous décidez d'essayer une nouvelle applicati on Internet durant les heures de pointe.

Jusqu'ici, la méthode des quatre inséparables vous a déjà fait rédiger quatre listes de données subjectives, de données objectives, d'analyse et de plan. Tout cela est bien long et fastidieux. Et pourtant, comme vous pouvez le constater, cette méthode est très intéressante pour affiner les informations que vous possédez déjà, ainsi que pour vous aider à émet tre des hypothèses, à les confirmer ou les infirmer. En définitive, cela vous permet de progresser.

Le lendemain. matin, vous essayez une nouvelle application Internet à 8 H 00 : elle fonctionne immédiatement. Certes, elle ne joue pas le même rôle que l'applet initiale, mais au moins, vous êtes bien en train de comparer des choses comparables - à savoir une applic ation conçue pour l'Internet, dépendante d'un firewall, et une autre application conçue pour l'Internet, elle aussi dépendante d'un firewall. Afin d'en avoir le coeur net, vous essayez une dernière application Internet, qui fonctionne elle aussi parfaitem ent. Voici la dernière liste que la méthode des quatre inséparables vous permet de rédiger

- Données subjectives. C'est l'applet elle -même qui semble être en cause.
- Données objectives. Vous n'avez essayé que deux autres applica tions Internet.
- Analyse. Il pourrait être utile de mesurer les retards d'achemine ment de données et le degré de saturation du réseau, mais quoi qu'il en soit, vous devrez faire appel au concepteur de l'applet.
- Plan. Vous contactez le concepteur de l'applet et vous lui commu niquez toutes les notes qui vous ont conduit à cette conclusion.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Fort heureusement, cette applet n'est pas un produit gratuit que vous avez découvert sur l'Internet. Son concepteur a à coeur de l'optimiser en fonction de votre réseau et de la faire fonctionner corr ectement pour vous. Il demande de lui communiquer des traces du réseau, que vous lui envoyez par courrier électronique. Sa réponse est que votre réseau est soumis à un trafic important, mais pas exagéré. Le grand nombre de notes que vous lui avez envoyées lui permet de se faire une idée relativement précise de la situation du réseau. Il en vient donc à penser que c'est probablement ce dernier qui pose problème. Souhai tant vous garder comme client, il vous envoie rapidement un patch pour le programme, par c ourrier électronique. Vous installez ce patch sur le PC de la personne qui vous avait signalé le problème et le tour est joué.

INFO
Dans un cas de figure tel que celui-là, veillez à documenter le problème -soit de manière informelle (en envoyant des messa ges électroniques à vos collègues), soit de manière formelle (en ajoutant un addendum à la documentation du produit dans votre bibliothèque technique). Vous pouvez écrire quelque chose du type

20/10/98, JF : l'applet ne fonctionne pas quand le réseau est très sollicité; pour remé
dier au problème, utiliser la patch 1.2, située sur le serveur "Barbares", dans le dossier "Patchs".

Illusoire, l'hypothèse selon laquelle un éditeur de logiciels tiendrait compte des remarques d'un client et apporterait les modifications qui s'imposent ? Pas vraiment. De fait, de plus en plus d'éditeurs de logiciels tiennent compte des remarques de leurs clients. Si vous suivez scrupuleusement les procédures de la méthode des quatre inséparables, vous avez plus de chances de convaincre le service technique de l'éditeur que vous êtes confronté à un problème qui mérite son attention. Il est d'ailleurs encore plus probable que vous trouviez la solution vous-même - ce qui était l'objectif initial.

XI-5- L'APPROCHE NAIVE

Comme nous l'avons vu dans le chapitre précédent, même si vous jouez le rôle de "docteur réseau", il est important que vous alliez vous-même consulter quand la situation semble désespérée. L'opération est simple, rapide et peu coûteuse. De surcroît, en soumettant votre réseau à un regard neuf, vous pouvez recueillir des observations auxquelles vous n'auriez pas pensé. Mieux encore, si vous vous décidez à exposer votre problème à quelqu'un d'autre, vous serez probablement contraint de réaliser un schéma pour décrire votre situation, mettre en évidence les points importants, etc. Cela vous permettra de mieux appréhender le problème vous-même.

Votre problème a déjà été résolu par quelqu'un d'autre
Ne serait-il pas intéressant de pouvoir consulter rapidement et facile ment un expert en réseaux ? Mieux encore, ne serait-il pas merveilleux que cette consultation soit gratuite ? Eh bien, sachez que ce rêve peut devenir réalité. La plupart des fabricants permettent d'effectuer des recherches portant sur des milliers de pages de documentation détaillée émanant de leur personnel d'assistance technique. Vous avez en fait accès au savoir des plus grands gourous du monde de l'informatique. Le meilleur moyen de ne pas avoir à réinventer la roue peut consister à interroger une base de données de connaissances ou d'informations techniques. Notam ment pour des problèmes d'interaction (un logiciel ou un périphérique donné en affecte un autre) ou de documentation lacunaire.

Cela semble presque trop beau pour être vrai. Pourquoi les fabr icants offrent-ils ces services au public ? Parce que, pour assurer une assistance technique efficace, les directeurs techniques ont besoin de bases de données bien conçues qui recensent tous les problèmes et les solutions apportées. C'est à eux-mêmes qu'ils cherchent à éviter de réinventer la roue en permanence. Ce système leur permet également de gagner un temps considérable (et par conséquent de réaliser des réductions de coûts tout aussi considérables). L'assistance technique est l'un des facteurs de fidélisation des clients. Les fabricants ont donc tout à gagner à rendre ces bases de données accessibles au public. En procé dant ainsi, les fabricants peuvent également réduire les coûts liés à l'assistance téléphonique gratuite qu'ils offrent -ils ont en permanence la possibilité de renvoyer leurs clients à la base de données de leur site Web. Dans ce cas aussi, l'assistance téléphonique est gratuite pour le client, même s'il doit payer les communications téléphoniques. L'inconvénient est toutefois que les sites Web de fabricants ne sont pas toujours

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

rédigés en français. Prévoyez un bon dictionnaire ou, mieux encore, demandez à votre entreprise de vous offrir des cours d'anglais pour rafraîchir vos connaissances !

INFO
Veillez à ne pas effectuer vos recherches à partir de la page d'accueil d'une entreprise. Les recherches effectuées à partir de la page d'accueil portent sur l'ensemble du site, et englobent des informations non techniques telles que des communiqués de presse. La plupart des entreprises possèdent, sur leur site Web, une page d'accueil de support technique qui ne contient que des informations techniques.

Les adresses de type **www.societe.com** ne permettent d'accéder qu'à la page d'accueil générale du site. La page d'accueil de support technique est généralement située à une adresse du type **support.societe.com** www.societe.com

INFO
D'une manière générale, plus les mots clés entrés pour une recherche sont nombreux, meilleur est le résultat de la recherche. Toutefois, quand ils sont trop nombreux, les résultats donnent l'impression d'être mal ciblés. A titre d'exemple, si vous spécifiez le mot clé erreur de carte réseau 78E8, vous risquez d'être envahi de documents contenant le mot "réseau". Il en ira de même des mots "carte" et "erreur". Dans ce cas, mieux vaut vous limiter à spécifier le mot clé 7E8.

Si le site offre un moteur de recherche plus sophistiqué, cette approche n'est pas indispensable. Ce moteur de recherche vous permettra de formuler votre recherche sous la forme

erreur de carte réseau + 78E8

ou

erreur de carte réseau" AND "78E8"

Ces deux critères de recherche signifient en clair: "ne me montre pas les documents parlant d'erreur de carte réseau s'ils ne contiennent pas 78E8".

Rechercher de l'aide de manière appropriée
En fait, vous êtes probablement aussi efficace pour interroger la base de données d'assistance technique d'un fabricant que l'opérateur de premier niveau qui répond au téléphone quand vous appelez le service d'assistante technique. Tout le problème est de savoir *quoi* et *où* chercher.

A titre d'exemple, supposez que vous ayez besoin de déployer Windows NT au sein de votre entreprise. En personne responsable et professionnelle, vous effectuez un test pilote sur votre réseau, afin d'affecter le moins de machines productives possible. A mi-chemin du déploiement, un utilisateur se plaint qu'il rencontre des problèmes quand il utilise la commande DOS EDIT et d'autres utilitaires DOS. Apparemment, l'ordinateur lui demande d'insérer une disquette dans le lecteur chaque fois qu'il exécute un programme DOS, même si l'opération en .cours ne nécessite pas de disquette. Voilà une situation pour le moins étrange. Vous vous demandez quel élément peut bien être différent des autres, et vous décidez d'aller sur l'ordinateur d'une autre personne. Vous effectuez la même opération en utilisant l'ordinateur et le nom d'utilisateur de cette autre personne et vous obtenez le même résultat.

Vous vous apercevez que tous les ordinateurs sur lesquels vous avez déployé Windows NT présentent ce problème. Vous interrompez, bien entendu, immédiatement le déploiement, mais vous n'en êtes pas moins confronté à un problème bien étrange. Pourquoi une machine qui vient d'être configurée se comporte-t-elle de la sorte ? En fait, tous les ordinateurs que vous avez installés vous-même présentent ce problème. S'agit-il d'une erreur de niveau matériel ou logiciel ? Si c'est une erreur de niveau logiciel, quel logiciel faut-il incriminer ? Et au fait, s'agit-il vraiment d'un problème de réseau ?

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Beaucoup de paramètres peuvent être complètement erronés dans ce type de situation. Il est temps de consacrer quelques minutes à une petite recherche. Fort heureusement, vous avez sous les yeux l'élément à rechercher, qui se présente sous la forme d'un message assez désagréable :

NTVDM : pas de disquette. Veuillez insérer une disquette dans le lecteur A:

Le premier site de recherche qui vous vient à l'esprit est, bien entendu, celui de Microsoft, qui préconise de contrôler le chemin de fichiers de Windows NT pour déterminer s'il fait référence au lecteur A, ce qui n'est pas le cas sur votre réseau.

Pour mieux cibler les sites sur lesquels vous pouvez espérer des réponses, prenez le temps de passer en revue les éléments que vous avez ajoutés au nouvel ordinateur :

- Windows NT ;
- Antivirus Intel ;
- WordPerfect Suite 8 ;
- GroupWise (logiciel de courrier électronique et de planification de groupe).

Tout à coup, vous vous ravisez : vous avez négligé au moins deux aspects du problème. Vous avez pensé aux logiciels d'application, mais en fait, il y a d'autres paramètres à prendre en considération. Vous décidez donc de tout reprendre depuis le début et de dresser la liste de toutes les étapes d'installation de cet ordinateur. Les facteurs sources - que vous aviez négligés - pouvant être causes de problèmes apparaissent en gras dans la liste suivante :

- Déballage du PC Dell ;
- Installation de base déjà effectuée ; Windows NT et le Service Pack 3 préinstallés ;
- Installation de Novell IntranetWare Client32 (nécessaire pour se connecter à un serveur Novell) ;
- Configuration de la carte réseau Ethernet 3Com ;
- Installation de l'antivirus Intel Virus Protection, de Corel WordPerfect Suite 8 et de Novell GroupWare.

Au terme de cette énumération des opérations effectuées sur la station de travail, vous disposez d'une liste de fabricants dont vous pouvez consulter les sites Web. Votre liste finale de points de recherche contient les éléments suivants

- Dell ;
- Microsoft ;
- Novell ;
- Intel ;
- Corel.

Au lieu de réinstaller un nouveau PC, ce qui risque de prendre une heure ou deux (si tout se passe correctement!) vous décidez d'aller visiter les sites Web suivants et d'utiliser le message qui s'affiche sur votre écran comme mots clés :

- http://support.dell.com
- http://support.microsoft.com
- http://support.novell.com
- http://support.3com.com
- http://support.corel.com

Vous pouvez commencez par entrer le sigle "NTVDM" lui-même, car il s'agit d'un terme unique. Une fois encore, il ne rime à rien de demander à accéder aux documents contenant des mots clés tels que "insérer" et "disquette", car ce sont des mots très employés dans quantité de domaines. (N'oubliez pas que si vous n'affectez pas des degrés de priorité aux différents mots clés-ce que ne permettent pas de faire tous les sites de fabricants-le moteur de recherche retiendra tous les

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

documents contenant un ou plusieurs de ces mots clés. Ainsi, si vous entrez "insérer disquette NTVDM", le moteur de recherche retiendra beaucoup plus de documents pour les mots cles "insérer" et "disquette" que pour "NTVDM".) De plus, "NTVDM" est un sigle anglais, ce qui vous donne plus de chances d'arriver à vos fins sur un site Web anglophone.

Le moteur de recherche de Dell ne trouve rien pour "NTVDM". Le site Web de Microsoft contient des millions de documents d'information, et le mot clé "NTVDM" lui-même fait apparaître près de 100 documents. Vous vous dites que vous reviendrez sur cette page si vous ne trouvez pas de solution plus satisfaisante. Au troisième essai, sur le site de Novell, vous trouvez enfin les informations dont vous avez besoin. Comme vous pouvez le voir sur la Figure 7.1, une recherche ciblée sur "NTVDM" ne fait apparaître que onze documents, ce qui est tout à fait surmontable. Un coup d'oeil au titre des entrées trouvées vous permet de localiser un document technique qui décrit précisément votre problème. Vous cliquez sur ce lien pour en savoir plus. Dans ce cas, vous découvrez que quand Novell Client32 est utilisé avec Windows NT et le Service Pack 3, qui présente un bogue, le problème apparaît. La documentation indique également une solution (consistant à copier le fichier NTDOS. SYS du CD-ROM original de Windows NT vers le répertoire C: \WINNT\SYSTEM de l'ordinateur).

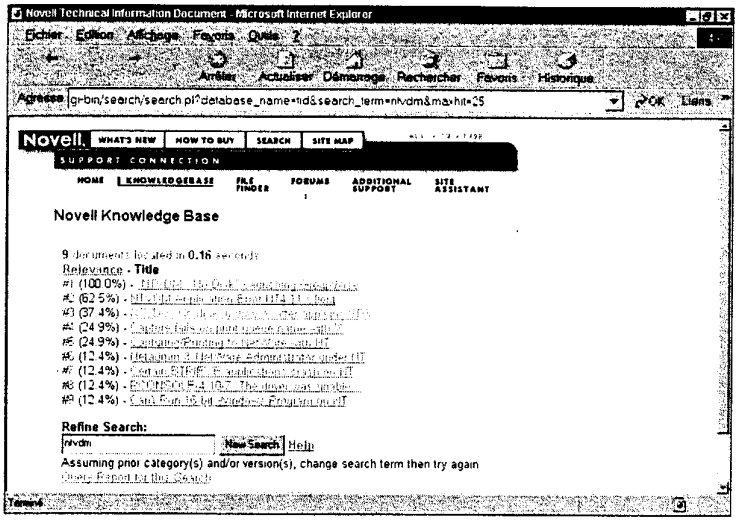


Figure 7.1
Il est généralement plus intéressant d'effectuer des recherches sur plusieurs sites que de s'attarder sur un même site.

ASTUCE
Quand vous devez résoudre un problème qui risque d'impliquer plusieurs marques de matériel, ne vous attardez pas trop sur chaque site - un fabricant peut proposer une solution immédiate, ou au contraire passer par des centaines de documents avant de trouver une soluti on viable.

Cinq minutes après avoir lancé votre navigateur Web, vous avez résolu le problème. Formidable ! Vous auriez pu passer des heures à diviser pour régner si vous n'aviez pas bénéficié de la puissance des techniques Internet.

Utiliser les forums pour obtenir de l'aide
Ne sous-estimez pas la puissance des forums publics. Les groupes de discussion Usenet et les listes de diffusion peuvent être extrêmement utiles pour obtenir de l'aide. Tous les fabricants n'offrent pas de forums sur leur propre site Web, car le service Usenet est parfois vecteur de propos peu flatteurs pour eux. (Il n'est pas rare de tomber sur des messages disant par exemple : "Ce produit est une vraie pourriture" !). Les fabricants tendent également à fuir les groupes de discussion Usenet et les listes de diffusion extérieures, car ils ne peuvent exercer aucun contrôle éditorial sur les messages publiés. Néanmoins, ces forums sont souvent source d'informations tirées de l'expérience bien réelle d'autres utilisateurs - des informations qu'il est souvent impossible d'obtenir du fabricant. Toutefois, force est de reconnaître qu'il faut souvent

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

brasser des quantités d'informations totalement sans intérêt avant de trouver une information vraiment utile.

ASTUCE
N'oubliez pas de commencer par faire des recherches sur le site d'assistance technique des différents fabricants concernés, avant de vous lancer dans une rechercher portant sur l'ensemble du Web. Cette approche vous permettra souvent de gagner du temps.

La plupart des moteurs de recherche Web (AltaVista, Lycos, etc.) permettent de faire porter la recherche sur Usenet plutôt que sur les pages Web. Toutefois, vous avez sans doute intérêt à opter pour un moteur de recherche spécialisé dans les groupes de discussion, comme **www.dejanews.com.** Ce type de service permet d'effectuer des recherches plus précises et de les limiter aux messages publiés récemment.

Fort heureusement, vous pouvez aussi effectuer des recherches sur Usenet. Si votre fournisseur d'accès ne vous permet pas d'accéder aux groupes de discussion Usenet, ou si votre application de groupes de nouvelles ne permet pas d'effectuer des recherches, vous pouvez utiliser des moteurs de recherche basés sur le Web pour trouver une rubrique d'aide ou un message d'erreur précis.

En plus des groupes Usenet et des listes de diffusion, certains fabricants et certains revendeurs proposent gratuitement leur propre forum sur le Web. Ces forums sont généralement relativement intéressant car, en plus des informations apportées par le public, ils offrent une assistance technique assurée par des techniciens professionnels. Bien que les fabricants ne soient pas tenus de répondre aux questions posées sur les forums publics, les services d'assistance technique ne laissent généralement pas les problèmes légitimes sans réponse - ils ont tout intérêt à ce que le public puisse utiliser leurs produits sans problèmes (voir Figure 7.2).

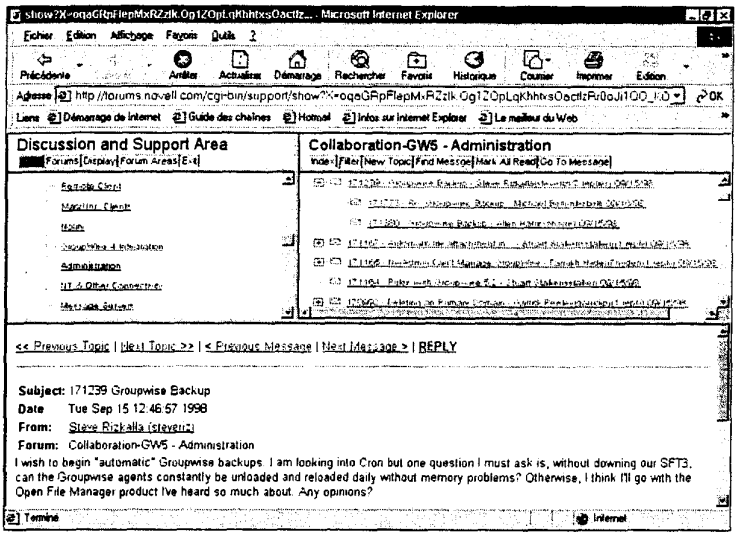


Figure 7.2
Le forum Web de Novell en action.

Certaines sociétés tierces proposent également des forums, dont elles se servent comme supports publicitaires. L'intérêt est que ces sociétés sont généralement impartiales quant aux produits dont il est question. Leur seule préoccupation est que ces produits répondent aux besoins de leurs utilisateurs. Une fois encore, votre propre expérience peut vous amener à avoir un avis différent sur ces forums. La Figure 7.3 montre un exemple de forum consacré à Windows NT.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

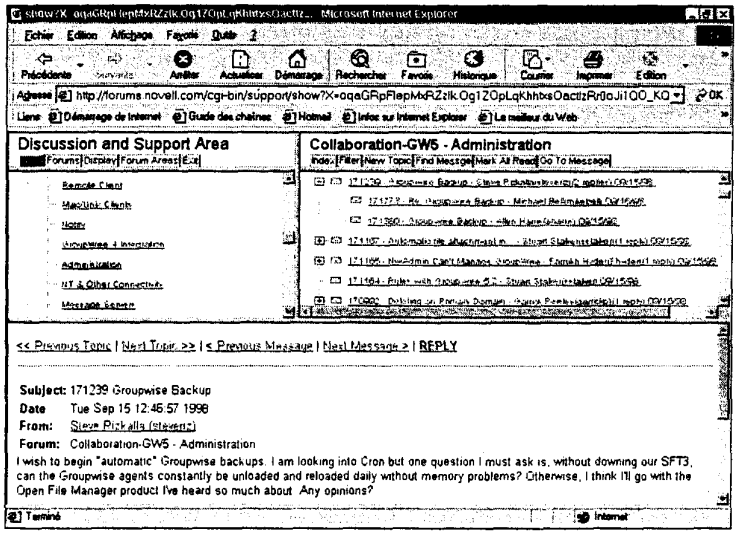

Discussion and Support Area
Collaboration-GW5 - Administration
<< Previous Topic | Next Topic >> | < Previous Message | Next Message > | REPLY
Subject: 171239 Groupwise Backup
Date Tue Sep 15 12:46:57 1998
From: Steve Pickalla (steveprj)
Forum: Collaboration-GW5 - Administration
I wish to begin "automatic" Groupwise backups. I am looking into Cron but one question I must ask is, without downing our SFT3, can the Groupwise agents constantly be unloaded and reloaded daily without memory problems? Otherwise, I think I'll go with the Open File Manager product I've heard so much about. Any opinions?

Figure 7.3
Un site d'assistance pour Windows NT proposé par une société tierce.

CD-ROM d'assistance technique

Tant que l'assistance technique est gratuite, les obligations du fabricant restent modestes. Si vous êtes tenace, vous pouvez espérer forcer un fabricant apparemment mal disposé à votre égard à vous venir en aide. Néanmoins, dans certains cas, vous devrez absolument investir dans un CD-ROM contenant une base de connaissances techniques pour obtenir une solution à un problème.

Certaines bases de connaissances basées sur le Web, comme celle de Microsoft, sont si sollicitées qu'il peut être insupportable de devoir attendre si longtemps le téléchargement de chaque page. Dans ce cas, vous pouvez, pour quelques centaines de francs, vous abonner au produit TechNet de Microsoft. Que vous aimiez ou que vous haïssiez Microsoft, vous aimerez TechNet. Comme la plupart des bases de connaissances sur CD-ROM, TechNet offre à l'utilisateur des fonctions très évoluées, qui permettent d'accéder beaucoup plus rapidement aux informations. Avec TechNet, vous pouvez par exemple affiner le résultat de vos recherches par produit, puis marquer la rubrique de résultats à l'aide d'un signet. Les informations techniques contenues dans TechNet sont disponibles dix fois plus rapidement sur le Web (voir Figure 7.4).

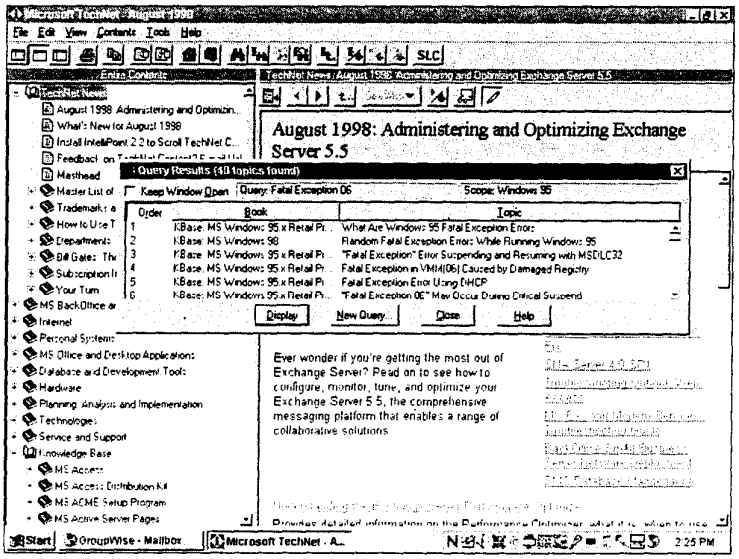

August 1998: Administering and Optimizing Exchange Server 5.5
Query Results (10 topics found)
Ever wonder if you're getting the most out of Exchange Server? Read on to see how to configure, monitor, tune, and optimize your Exchange Server 5.5, the comprehensive messaging platform that enables a range of collaborative solutions.

***Figure** 7.4*
Une session Microsoft TechNet.

ASTUCE

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Pour convaincre votre chef de service de l'utilité d'acheter TechNet, expliquez -lui que ce produit ne coûte pas plus cher qu'une ou deux séances d'assistance technique payante par téléphone, ou qu'une bu deux visites de votre consultant en réseaux.

INFO

Bien entendu, si le problème reste insoluble au bout d'un intervalle de temps raisonna ble, vous devrez vous résoudre à chercher de l'aide à l'extérieur. Chacun sait que "le temps, c'est de l'argent", et ce dicton est plus pertinent que jamais quand ce temps correspond, dans une entreprise, à une période de non-productivité provoquée par une panne de réseau. Une visite de quelques heures d'un consultant peut représenter un investissement très rentable si elle vous permet, en contrepartie, d'économiser une dizaine d'heures de travail alors qu'un composant stratégique de votre réseau est en panne. Si vous devez, en définitive, payer pour obtenir une aide ex térieure, consolez vous en vous disant que le temps ainsi gagné sera très utile à votre entreprise. Le travail de dépannage que vous avez effectué (et que vous continuerez d'effectuer) sur le réseau a déjà permis à votre entreprise de réaliser des économie s importantes, puisque vous avez fortement dégrossi le travail du consultant.

La "Rolls" des bases de données d'assistance technique, le produit Support Source de MicroHouse, coûte près de 5 000 F pour un abonnement d'un an. Réfléchissez à deux fois avan t d'investir dans un produit tel que celui-ci, d'autant qu'il n'est pas actuellement disponible en français. Certes, les ressources de ce type offrent des informations qui ont été sélectionnées très soigneusement ; elles s'appuient sur de nombreuses sources d'assistance technique et sont tout simplement fantastiques pour les professionnels qui ont besoin de réponses très rapides. Néanmoins, vous devez vous demander à quelle fréquence vous pensez utiliser ce type de produit. Les bases de données de ce type contiennent une pléthore de communiqués de presse et de cours tech niques, assortis d'un système de recherche très pratique. Cependant, vous pouvez parfaitement obtenir des informations similaires en recou rant à un moteur de recherche basé sur le Web (voir Figure 7.5). A moins que vous ne soyez très souvent appelé à dépanner le réseau de votre entreprise (auquel cas vous êtes en droit de demander une augmentation de salaire à votre patron), ce type d'investissement ne se justifie pas forcément.

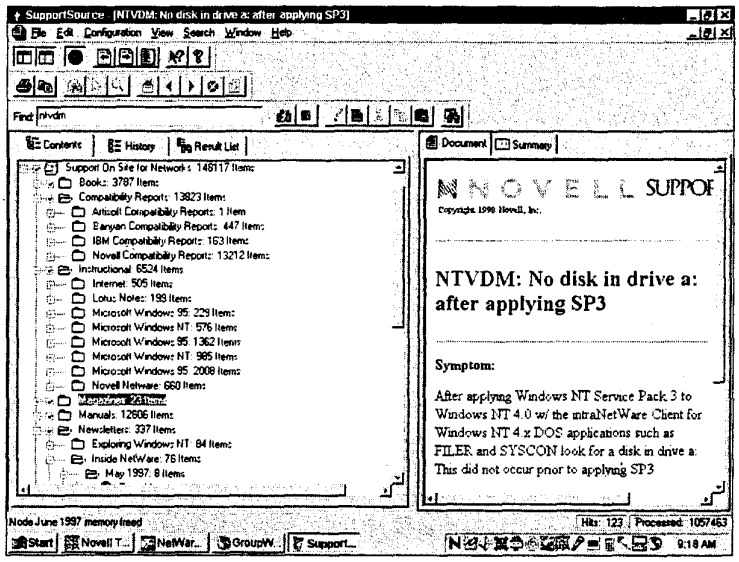

SupportSource [NTVDM: No disk in drive a: after applying SP3]
File Edit Configuration View Search Window Help
Find: ntvdm
Contents
History
Result List
Document
Summary
Support On Site for Networks 148117 Items
Books: 3787 Items
Compatibility Reports: 13823 Items
Artisoft Compatibility Reports: 1 Item
Banyan Compatibility Reports: 447 Items
IBM Compatibility Reports: 163 Items
Novell Compatibility Reports: 13212 Items
Instructional 6524 Items
Internet: 505 Items
Lotus Notes: 199 Items
Microsoft Windows 95: 229 Items
Microsoft Windows NT: 576 Items
Microsoft Windows 95: 1362 Items
Microsoft Windows NT: 985 Items
Microsoft Windows 95: 2008 Items
Novell Netware: 660 Items
Manuals: 12606 Items
Newsletters: 337 Items
Exploring Windows NT: 84 Items
Inside NetWare: 76 Items
May 1997: 8 Items
NOVELL SUPPOR
Copyright 1996 Novell, Inc.
NTVDM: No disk in drive a: after applying SP3
Symptom:
After applying Windows NT Service Pack 3 to Windows NT 4.0 w/ the intraNetWare Client for Windows NT 4.x DOS applications such as FILER and SYSCON look for a disk in drive a: This did not occur prior to applying SP3
Node June 1997 memory freed
Hits: 123 Processed: 1057453
Start
Novell T...
NetWar...
GroupW...
Support...
9:18 AM

Figure 7.5
Session de recherche sous Support House, de MicroHouse.

Co-dépendance

Si vous avez lu attentivement ce livre, étudié la documentation du fabricant et consulté les bases de données, et si vous êtes toujours bloqué, il est temps d'appeler directement le fabricant. Que vous deviez payer pour convaincre un spécialiste de v enir examiner un problème qui semble désespéré à votre niveau, ou que vous deviez souscrire un contrat d'assistance technique, vous pouvez appliquer un certain nombre de stratégies pour tirer le maximum de votre rencontre avec ce spécialiste.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Votre premier effort, qui appartient en principe désormais au passé, consiste à documenter correctement le problème pendant la phase de dépannage. Si vous avez utilisé la méthode de dépannage des quatre inséparables en essayant de résoudre vous-même le problème, vous possédez normalement, d'ores et déjà, les informations dont le spécialiste a besoin pour analyser la situation. Ainsi, vous êtes en mesure de lui indiquer :

- le type du matériel concerné ;
- le type du réseau concerné ;
- les applications concernées ;
- quand le problème s'est manifesté (heure d'apparition, durée) ;
- si le problème peut être reproduit.

INFO
Si vous ne pouvez pas reproduire le problème, votre interlocuteur téléphonique ne pourra pas le reproduire non plus. A l'inverse, si vous parvenez à le reprod uire sur une autre station de travail ou sur un serveur, vous serez vraiment en mesure de convaincre le service d'assistance technique que votre problème est réel et qu'il n'est pas dû à votre environnement de réseau.

Les personnes qui se précipitent sur le service d'assistance technique, sans avoir au préalable réuni les informations nécessaires, sont généralement reçues fraîchement par celui-ci. (Or, paradoxalement, quand vous vous êtes donné la peine de rechercher ces informations, la source du problème devient souvent évidente et vous n'avez plus besoin d'appeler le service d'assistance technique.) Ainsi, quand un technicien voit que son interlocuteur n'a pas fait l'effort de rechercher les informations dont il a besoin pour effectuer un diagnostic, il a tendance à rejeter la faute sur un autre fabricant (stratégie puérile et irresponsable du "c'est pas moi, c'est lui !"). Si vous avez contacté le fabricant de votre carte réseau, par exemple, il vous renverra sur le fabricant du système d'exploitation de réseau. Or, il est généralement difficile de réfuter l'avis d'un technicien qui prétend que le problème ne relève pas de lui, mais du service d'assistance technique d'un autre fabricant.

Vous pouvez lutter contre ce type de comportement en vous munissant d'une preuve documentée que vous pourrez présenter au fabricant apparemment mal disposé à votre égard - le service d'assistance technique peut vous indiquer, par téléphone, comment vous. constituer cette preuve. Vous pouvez en effet réaliser un test par vos propres moyens. Comme vous le verrez au Chapitre 17, il n'est pas nécessaire d'être un expert pour être en mesure de soumettre des traces de réseau à un service d'assistance technique. Les traces de réseau sont, en substance, des statistiques détaillant point par point ce qui se passe dans le câble du réseau. Elle peuvent être très utiles à l'expert en réseau que vous aurez au téléphone.

Une autre manière de lutter contre cette tendance qu'ont certains fabricants à rejeter la faute sur autrui consiste à réitérer le problème manuellement, sans faire intervenir l'élément que le technicien que vous avez eu en ligne désigne comme fautif. En d'autres termes, si un programme affiche systématiquement un message d'erreur signalant qu'il ne peut pas écrire sur le serveur alors que vous pensez qu'il le devrait, essayez d'enregistrer vous-même un fichier sur le serveur avec le même nom d'utilisateur et durant la même session (ne réinitialisez pas l'ordinateur et ne fermez pas la session en cours). En d'autres termes, si le programme indique :

Impossible de copier "FOO.EXE" de D:\setup\foo à G:\monapp. Réessayer ?

vous pouvez toujours essayer de réaliser la même opération manuellement depuis la ligne de commande de MS-DOS, en tapant

C:\> COPY D:\setup\foo G:\monapp

Vous pouvez également utiliser l'Explorateur de Windows pour essayer de copier le fichier **FOO.REXE** de D: \setup\foo à G: \monapp.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Un même fabricant peut fort bien offrir à la fois une assistance techni que très efficace et un site Web très complet. L'expérience montre que cela existe ! Néanmoins, force est de constater que de tels fabricants sont rares. Si vous avez la chance d'en rencontrer, achetez-lui autant de produits que vous le pouvez et priez très fort pour qu'il ne change pas de stratégie avec le temps ! Plus sérieusement, les techniciens des services d'assistance technique peuvent réellement être d'une aide très précieuse pour résoudre des problèmes. Il ne faut donc pas hésiter à les appeler en cas de besoin.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

XII- DEMARCHE METHODOLOGIQUE DE RESOLUTION DES PROBLEME DES RESEAUX LOCAUX

XII-1 METHODE SCIENTIFIQUE

Le dépannage de réseau consiste en la mise en application d'une procédure systématique afin de résoudre un problème sur un réseau. L'utilisation de la matrice de conception de Dartmouth, dont vous vous êtes servi dans la partie du cours traitant de la conception d'un réseau, permet de démarrer de façon efficace. Cet outil est très utile pour établir une technique d'analyse systématique à des fins de dépannage. Une autre technique à utiliser est la méthode scientifique. La première liste décrit la méthode scientifique réelle et la deuxième indique son application pour le dépannage.

Méthode scientifique

1. Observez un certain aspect de l'univers.
2. Elaborez une théorie qui est conforme à ce que vous avez observé.
3. Faites des prédictions en vous fondant sur cette théorie.
4. Mettez ces prédictions à l'épreuve au moyen d'expériences ou d'autres observations.
5. Modifiez la théorie à la lumière de vos résultats.
6. Retournez à l'étape 3.

Méthode scientifique appliquée au dépannage :

1. Déterminez le problème touchant le réseau ou un utilisateur.
2. Recueillez des données sur ce problème.
3. Analysez les données afin de trouver une solution possible au problème.
4. Mettez la solution en oeuvre sur le réseau afin de tenter de corriger le problème.
5. Si le problème n'est pas résolu, annulez les changements que vous venez d'effectuer et modifiez les données.
6. Retournez à l'étape 3.

XII-2 ANALYSE POUR LE DEPANNAGE DE RESEAU

Voici un exemple de cette méthode de dépannage : un utilisateur de votre réseau appelle le service de dépannage pour signaler que son ordinateur n'a plus accès à Internet. Le service de dépannage remplit un relevé d'erreur qu'il envoie au service chargé du soutien du r éseau, c'est-à-dire vous.

Vous appelez l'utilisateur. Ce dernier indique qu'il n'a rien fait de différent pour avoir accès à Internet. Vous vérifiez les journaux relatifs au matériel du réseau et découvrez qu'une mise à niveau de l'ordinateur de l'utilisateur a été effectuée la veille. La première hypothèse est que les pilotes réseau ont été configurés incorrectement. Vous vous rendez à l'ordinateur et vérifiez l'information de configuration réseau qui s'y trouve. Comme elle semble correcte, vous envoyez u ne requête Ping au serveur sur ce sous-réseau. Aucune connexion n'est établie.

La prochaine hypothèse consiste à vérifier si le câble du poste de travail est branché. Vous vérifiez les deux extrémités du câble et lancez de nouveau la requête Ping. Il n'y a toujours pas de connexion.

Vous lancez ensuite une commande Ping à l'adresse 127.0.0.1, soit l'adresse de l'essai en mode bouclé pour l'ordinateur. Comme la commande Ping s'exécute correctement, vous pouvez éliminer l'ordinateur, la configuration des pilotes et la carte réseau comme causes possibles du problème.

Vous déterminez qu'il peut y avoir un problème avec le serveur pour ce segment du réseau. Un autre ordinateur relié au réseau se trouve sur le bureau d'à côté. Vous lancez une requête Ping à l'adre sse du serveur. Elle s'exécute correctement. Vous pouvez ainsi éliminer le serveur, le réseau fédérateur et la connexion du serveur à ce dernier comme causes possibles du problème.

Vous vous rendez au répartiteur intermédiaire et commutez le port du poste de travail, revenez au poste de travail et lancez de nouveau une requête Ping au serveur. Cette solution ne fonctionne pas. Votre recherche se concentre maintenant sur le câblage horizontal et le câble de raccordement du poste

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

de travail. Vous retournez au répartiteur intermédiaire, connectez de nouveau le câble sur le port de commutation qu'il occupait précédemment, obtenez un nouveau câble de raccordement et revenez au poste de travail.

Vous remplacez le câble du poste de travail et lancez de nouveau une requête Ping au serveur. Cette fois-ci, elle s'exécute correctement. Vous avez donc résolu le problème.

La dernière étape consiste à indiquer la solution du problème sur le relevé d'erreur et à retourner ce dernier au service de dépannage. Celui-ci consigne la résolution du problème.

Comme vous avez pu le constater, cet exemple explique chaque étape du travail à faire pour éliminer les causes possibles d'un problème sur le réseau. Dans l'exemple, vous avez traité et éliminé chaque problème possible. Si vous effectuez plusieurs modifications en une seule fois, le processus peut devenir confus et il devient impossible de définir la solution avec précision. Au fur et à mesure que des solutions étaient mises en œuvre sans pouvoir résoudre le problème, vous avez réévalué les données et trouvé de nouvelles solutions possibles. Ce processus s'est poursuivi jusqu'à ce que vous ayez trouvé la cause réelle du problème et résolu ce dernier. Vous avez ensuite consigné le problème à des fins de consultation ultérieure.

Peu importe le type de problème pouvant survenir sur un système de réseau, la procédure pour le résoudre est toujours la même. Elle a été décrite précédemment dans ce chapitre.

XII-3- DEPANNAGE DE RESEAUX

Résolution de problèmes

Les problèmes sont inévitables. Même dans un réseau contrôlé, avec de l'équipement fiable et des utilisateurs prudents, des incidents peuvent survenir. Un bon administrateur réseau doit démontrer qu'il peut analyser, dépanner et résoudre des problèmes alors qu'il subit la pression d'une défaillance du réseau pouvant interrompre les activités de l'entreprise. Des techniques efficaces de gestion de réseaux ont été décrites au cours de la 3e session. Les suggestions ci-dessous constituent une révision de ces techniques et proposent d'autres outils pour assurer le dépannage d'un réseau. Voici donc un bref examen de techniques que nous avons vues précédemment et d'autres méthodes de dépannage. Comme nous l'avons déjà indiqué plus tôt, ces techniques peuvent constituer les meilleurs moyens de résoudre les problèmes sur un réseau. [1]

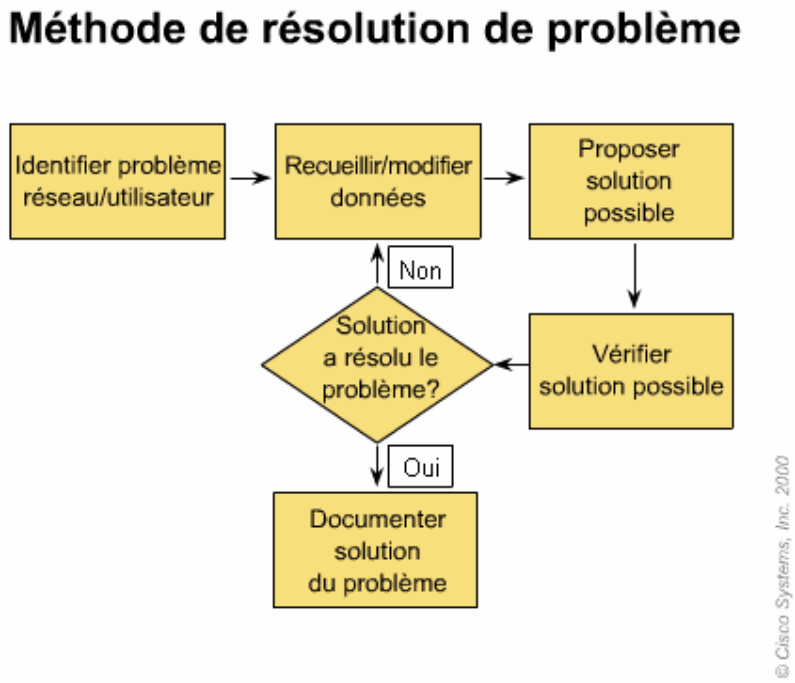
La première étape, et la plus importante, consiste à prendre des notes dans votre journal technique. Ces notes peuvent faciliter le diagnostic d'un problème. Elles peuvent vous indiquer les mesures déjà prises et leurs résultats par rapport au problème. Cette information peut être très précieuse pour le responsable du dépannage, car elle permet de ne pas répéter inutilement ces tentatives antérieures . Ces notes peuvent être également très utiles si le problème est confié à un autre technicien, pour qu'il n'ait pas à répéter le travail déjà accompli. Il faut inclure une copie de ces notes dans la solution du problème, lorsque le dossier du problème est clos. Cette information peut servir de référence si des problèmes similaires se produisent. [2]

L'étiquetage constitue une autre élément essentiel du dépannage préemptif. Etiquetez tout, y compris les deux extrémités d'un câble horizontal. Il faut indiquer sur l'étiquette non seulement le numéro du câble mais également l'emplacement de l'autre extrémité et l'utilisation du câble, par exemple pour la communication voix, données ou vidéo. Ce type d'étiquette peut s'avérer plus utile qu'une feuille d'identification des câbles pour le dépannage, car l'information se trouve au même endroit que l'unité et non pas dans un tiroir de classeur. En plus des câbles, l'étiquetage de chaque port d'un concentrateur, d'un commutateur ou d'un routeur afin d'en indiquer l'emplacement, l'utilisation et le point de connexion facilite grandement la résolution des problèmes. Enfin, il faut également munir tous les autres éléments reliés au réseau d'étiquettes indiquant leur emplacement et leur rôle. Ce type d'étiquetage permet de repérer facilement tous les éléments du réseau et de connaître leur rôle. L'utilisation d'un étiquetage approprié et de la documentation produite lors de la création et de la mise à jour du réseau permet d'obtenir une vue complète du réseau et de ses connexions. Voici un autre point important de la session précédente dont il faut se rappeler : la documentation n'est utile que dans

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

la mesure où elle est à jour. Il faut documenter tous les changements apportés au réseau, autant sur les unités ou les câbles modifiés que dans la documentation papier servant à définir l'ensemble du réseau.

La première étape du dépannage de réseau consiste à définir le problème. Cette définition peut regrouper des renseignements provenant de nombreuses sources différentes. Parmi ces sources, mentionnons un rapport d'incident ou un rapport du service de dépannage, qui fait état du problème pour la première fois. Une autre source peut être une conversation téléphonique avec l'utilisateur aux prises avec le problème, dans le but d'obtenir plus de renseignements sur l'incident. Les outils de surveillance du réseau peuvent donner un aperçu plus complet du problème précis à résoudre. Des observations d'autres utilisateurs et les vôtres constituent également des renseignements utiles. En évaluant toute cette information, la personne chargée du dépannage peut dégager avec plus de précision un point de départ pour la résolution du problème plutôt que de travailler à partir d'une seule de ces sources.



Méthodes de dépannage

Les deux techniques de dépannage réseau les plus efficaces sont le processus d'élimination et la méthode "diviser pour régner". Les scénarios ci-dessous illustrent ces techniques.

La technique du processus d'élimination est utilisée pour résoudre le problème suivant :

Un utilisateur de votre réseau appelle le service de dépannage pour signaler que son ordinateur n'a plus accès à Internet. Le service de dépannage remplit un relevé d'erreur qu'il envoie au service chargé du soutien du réseau, c'est-à-dire vous.

Vous appelez l'utilisateur. Ce dernier indique qu'il n'a rien fait de différent de ce qu'il fait habituellement pour avoir accès à Internet. Vous vérifiez les journaux relatifs au matériel du réseau et découvrez qu'une mise à niveau de l'ordinateur de l'utilisateur a été effectuée la veille. La première hypothèse est que les pilotes réseau ont été configurés incorrectement. Vous vous rendez à l'ordinateur et vérifiez l'information de configuration réseau qui s'y trouve. Comme elle semble correcte, vous envoyez une requête Ping au serveur sur ce sous-réseau. Aucune connexion n'est établie.

La prochaine hypothèse consiste à vérifier si le câble du poste de travail est branché. Vous vérifiez les deux extrémités du câble et lancez de nouveau la requête Ping. Il n'y a toujours pas de connexion.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Vous lancez ensuite une commande Ping à l'adresse 127.0.0.1, soit l'adresse d'essai en mode bouclé pour l'ordinateur. Comme la commande Ping s'exécute correctement, vous pouvez éliminer l'ordinateur, la configuration des pilotes et la carte réseau comme causes possibles du problème.

Vous déterminez qu'il pourrait y avoir un problème avec le serveur pour ce segment du réseau. Un autre ordinateur relié au réseau se trouve sur le bureau d'à côté. Vous lancez une requête Ping à l'adresse du serveur. Elle s'exécute correctement. Vous pouvez ainsi éliminer le serveur, le réseau fédérateur et la connexion du serveur à ce dernier comme causes possibles du problème.

Vous vous rendez au répartiteur intermédiaire et commutez le port du poste de travail, revenez au poste de travail et lancez de nouveau une requête Ping au serveur. Cette solution ne fonctionne pas. Votre recherche se concentre maintenant sur le câblage horizontal et le câble de raccordement du poste de travail. Vous retournez au répartiteur intermédiaire, connectez de nouveau le câble sur le port de commutation qu'il occupait précédemment, obtenez un nouveau câble de raccordement et revenez au poste de travail.

Vous remplacez le câble du poste de travail et lancez de nouveau une requête Ping au serveur. Cette fois-ci, elle s'exécute correctement. Vous avez donc résolu le problème.

La dernière étape consiste à indiquer la solution du problème sur le relevé d'erreur et à retourner ce dernier au service de dépannage. Celui-ci consigne la résolution du problème.

XII-4- MAINTENANCE DES RESSOURCES PARTAGEES

Impossible de trouver des Imprimantes par les emplacements
Vérifiez que l'emplacement utilise bien la bonne convention, qu'il est bien renseigné coté imprimante, mais aussi coté objet Active Directory.

Impossible d'accéder à un dossier visible dans une recherche Active Directory
Vous ne devez pas avoir les droits au niveau partage ou NTFS pour accéder à la ressource.

Un document reste bloqué dans la file d'attente d'une imprimante, Il ne s'imprime pas et on ne peut pas le supprimer
Redémarrez le service spooler sur le serveur d'impression. Ceci va supprimer tous les documents en attente.

Un périphérique d'impression est en panne, et plusieurs documents sont en attente dans la file
Ajoutez un nouveau port sur l'imprimante de type local Cette manipulation va rediriger tous les documents en attente vers le nouveau port.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

Module : Dépannage de premier niveau d'un réseau local

GUIDE DES TRAVAUX PRATIQUES

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

ATELIER #1

Principes de base du protocole TCP/IP

Objectifs visés

1. Assigner des adresses IP privée compatibles à chaque pair d'ordinateurs.
   a.) 10.14.59.xxx – masque : 255.0.0.0
   b.) 192.29.92.xxx – masque : 255.255.255.0

Préalable :

Notez votre adresse IP : _____
Utilisez l'une des commandes suivantes selon le SE utilisé
Windows NT : Dans une fenêtre Commande MS-DOS à ipconfig
Windows 9x : Démarrer / Exécuter à winipcfg

Configuration n°1

But : Connecter deux ordinateurs en utilisant un câble inversé

- Assigner une adresse IP privée au hasard à chaque ordinateur
- Le prof fourni 2 adresses IP

Configuration n°2

- Y a t il des changements ?
  Rép. on ne peut pas utiliser les mêmes câbles sauf s'il est branché au HUB dans une prise non renversée !
- On fournit des câbles direct.
  Y a t il des changements ?

Configuration no3

Donne 2 nouvelles adresses IP dans le réseau A
Rép. Tous les ordinateurs se voient

Procédure

Aller sur le PC voir et noter l'adresse IP :
dans le Panneau de configuration\Réseau\Protocols\TCP/IP Protocol (Win 9x/NT)

Ouvrir une fenetre DOS et faire PING pour vérifier la connection entre les P C A et B - C et D

Installer le HUB et connecter les 4 PC

Ping PC A et B - C et D (les combinaisons PC AB et CD devraient encore ce voir
Avec le même cablage refaire les adresses IP d'un des groupes de PC AB ou CD et vérifier s'ils se voient

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
http://www.pdfmail.com

ATELIER #2

Installation et administration de Windows 2000 Serveur

Modalité

- Ce laboratoire devra se faire en équipe de deux, Vous devez répondre aux questions dans votre cahier de laboratoire. Ce laboratoire ne fera pas l'objet d'un rapport de laboratoire.

Objectifs

- Installer un Windows 2000 Serveur
- Administrer un réseau client/serveur sur Windows 2000 Serveur
- Comparer Windows 2000 Serveur à Windows NT 4 Serveur
- Comparer Windows 2000 Serveur à Windows 2000 Professionnel

Equipements

- Une station de travail Windows NT 4 Server
- Une station de travail Windows NT 4 Workstation
- Une station de travail Windows 2000 Professionnel
- Une station de travail Windows 98

Préparation individuelle

- **Lisez attentivement tout l'énoncé du laboratoire.**
- Répondez aux questions dans votre cahier de laboratoire. Vous devez taper toutes les réponses et imprimer le laboratoire final.

1ière étape : Vérification (création) des comptes sous Windows NT 4 Serveurs

tap. Ouvrez le gestionnaire des utilisateurs (User Manager for Domains) et vérifiez (créez) la liste d'utilisateurs suivante avec leurs critères :

Utilisateur	MARCELJE	TREMBLMI	TREPANJE	LAMOTHRE
Nom détaillé	Jean-Luc Marcelin	Micheline Tremblay	Jean Trépanier	Régis Lamothe
Description	Professeur	Professeur	Professeur	Professeur
Mot de passe	Prof	Prof	Prof	Prof
Confirmer le mot de passe	Prof	Prof	Prof	Prof
L'utilisateur doit changer de mot de passe à la prochaine ouverture de session	Non	Non	Non	Non
L'utilisateur ne peut pas changer de mot de passe	Non	Non	Non	Non
Le mot de passe n'expire jamais	Non	Non	Non	Non
Compte désactivé	Non	Non	Non	Non

Utilisateur	PARADIJU	LATULIAN	AUDETDA	LACROIKA	LEBEAUJE	LAPOINDA
Nom détaillé	Julie Paradis	André Latulippe	Dany Audet	Karine Lacroix	Jean-François Lebeau	Daniel Lapointe
Description	Etudiante	Etudiant	Etudiant	Etudiante	Etudiant	Etudiant
Mot de passe	Etu	Etu	Etu	Etu	Etu	Etu
Confirmer le mot de passe	Etu	Etu	Etu	Etu	Etu	Etu
L'utilisateur doit changer de mot de passe à la prochaine ouverture de session	Non	Non	Non	Non	Non	Non
L'utilisateur ne peut pas changer de mot de passe	Non	Non	Non	Non	Non	Non
Le mot de passe n'expire jamais	Non	Non	Non	Non	Non	Non
Compte désactivé	Non	Non	Non	Non	Non	Non

onai . Ouvrez le gestionnaire des utilisateurs et vérifiez (créez) la liste de groupes suivante avec leurs critères :

Nom de groupe	Professeurs	Etudiants	4318	4319	4320
Description	Professeurs du département	Etudiants du département	Etudiants du groupe 4318	Etudiants du groupe 4319	Etudiants du groupe 4320
Type	Local	Global	Global	Global	Global
Membre	LAMOTHRE MARCELJE TREMBLMI TREPANJE	AUDETDAN LACROIKA LAPOINDA LATULIAN LEBEAUJE PARADIJU	LAPOINDA LEBEAUJE	AUDETDAN LACROIKA	LATULIAN PARADIJU

2ième étape : Vérification de la connexion d'un client Windows 98 à un serveur Windows NT 4 Serveur

étap. Vérifiez que dans la boîte de dialogue *Propriétés de Mots de passe*, l'onglet *Profils utilisateurs*, que l'option *Les utilisateurs peuvent …* soit sélectionnée. Expliquez utilité de cette option.

étap. Etes-vous en mesure de vous connecter en tant que MARCELJE sur le serveur à partir de Windows 98 ?

pap. Dans *Réseau*, l'onglet *Identification*, modifiez le groupe de travail pour le nom de votre domaine.

ésea. Etes-vous en mesure de vous connecter en tant que MARCELJE sur le serveur à partir de Windows 98 ?

tesa. Citez *tous* les éléments essentiels pour qu'un client Windows 98 puisse se connecter au serveur.

3ième étape : Vérification de la connexion d'un client Windows NT Workstation à un serveur Windows NT 4 Serveur

étap. Ouvrez le gestionnaire du serveur (Server Manager) et ajoutez un ordinateur de source Windows NT Workstation. (Ecrire la procédure)

étap. Etes-vous en mesure de vous connecter en tant que MARCELJE sur le serveur à partir de Windows NT Workstation ?

tesp. Supprimez l'ordinateur que vous avez ajouté au point 3.1.1 à partir du serveur. (Ecrire la procédure)

)esp. Etes-vous en mesure de vous connecter en tant que MARCELJE sur le serveur à partir de Windows NT Workstation ?

tesp. Connectez-vous sur la machine Windows NT Workstation en tant que *Administrateur*. Ouvrez la boîte de dialogue *Réseau*. Cliquez sur *Modifier*. Et sélectionnez *Membre de*. Cliquez sur *Créer un compte d'ordinateur dans le domaine*. Répondez à la question (le nom d'utilisateur demandé) et expliquez.

Et . Etes-vous en mesure de vous connecter en tant que MARCELJE sur le serveur à partir de Windows NT Workstation ?

nes . Vérifiez le contenu du gestionnaire du serveur.

4ième étape : Mise à niveau vers Windows 2000 Serveur

étap. Quelles sont les conditions pour effectuer une mise à niveau vers Windows 2000 Serveur ?

étap. Procédez à l'installation. Prenez en notes tous les choix importants que vous faites.

5ième étape : Utilisation de la fenêtre MMC (Microsoft Management Control)

56eS. Lancez la commande *MMC*.

MCS. Dans le menu *Console*, cliquez sur *Ajouter/Supprimer un composant logiciel enfichable* puis cliquez sur le bouton *Ajouter*.

jout. Sélectionnez *Gestion de l'ordinateur*, puis cliquez sur *Ajouter*.

jout. Assurez-vous que l'option *L'ordinateur local* soit sélectionné puis cliquez sur le bouton *Terminer*. Cliquez sur le bouton *Fermer* puis *OK*.

Kuis. Enregistrez la console sous le nom de *Gestion de l'ordinateur* puis quitter.

6ième étape : Vérification des comptes utilisateurs sous Windows 2000 Serveur

étap. Ouvrez *Gestion de l'ordinateur* à partir du menu *Démarrer*.

uvre. Déployez *Gestion de l'ordinateur*, *Outils système*, puis *Utilisateurs et groupes locaux*.

ocau. Créez les utilisateurs et groupes suivants :

Utilisateur	MARCELJE	TREMBLMI	TREPANJE	LAMOTHRE
Nom détaillé	Jean-Luc Marcelin	Micheline Tremblay	Jean Trépanier	Régis Lamothe
Description	Professeur	Professeur	Professeur	Professeur
Mot de passe	Prof	Prof	Prof	Prof
Confirmer le mot de passe	Prof	Prof	Prof	Prof
L'utilisateur doit changer de mot de passe à la prochaine ouverture de session	Non	Non	Non	Non
L'utilisateur ne peut pas changer de mot de passe	Non	Non	Non	Non
Le mot de passe n'expire jamais	Non	Non	Non	Non
Compte désactivé	Non	Non	Non	Non

Utilisateur	PARADIJU	LATULIAN	AUDETDA	LACROIKA	LEBEAUJE	LAPOINDA
Nom détaillé	Julie Paradis	André Latulippe	Dany Audet	Karine Lacroix	Jean-François Lebeau	Daniel Lapointe
Description	Etudiante	Etudiant	Etudiant	Etudiante	Etudiant	Etudiant
Mot de passe	Etu	Etu	Etu	Etu	Etu	Etu
Confirmer le mot de passe	Etu	Etu	Etu	Etu	Etu	Etu
L'utilisateur doit changer de mot de passe à la prochaine ouverture de session	Non	Non	Non	Non	Non	Non
L'utilisateur ne peut pas changer de mot de passe	Non	Non	Non	Non	Non	Non
Le mot de passe n'expire jamais	Non	Non	Non	Non	Non	Non
Compte désactivé	Non	Non	Non	Non	Non	Non

Nom de groupe	Professeurs	Etudiants	4318	4319	4320
Description	Professeurs du département	Etudiants du département	Etudiants du groupe 4318	Etudiants du groupe 4319	Etudiants du groupe 4320
Membre	LAMOTHRE MARCELJE TREMBLMI TREPANJE	AUDETDAN LACROIKA LAPOINDA LATULIAN LEBEAUJE PARADIJU	LAPOINDA LEBEAUJE	AUDETDAN LACROIKA	LATULIAN PARADIJU

7iéme étape : Conversion vers le ACTIVE DIRECTORY

tap. La conversion du serveur vers le Active Directory nous permettra d'appliquer une administration à partir d'objet. Celle-ci se fera à l'aide de la commande *DCPROMO.EXE*.

tap. Sélectionnez *Contrôleur de domaine pour un nouveau domaine*. Comme il s'agit d'un nouveau contrôleur, vous voudrez créer une nouvelle arborescence de domaine.

tap. On vous invite à créer une nouvelle forêt d'arborescences de domaines. Indiquez *ARBREXYZ* où XYZ représente votre numéro d'ordinateur.

tap. On vous demande un nom DNS complet pour le nouveau domaine. Indiquez *DOMAINEXYZ.COM*, où XYZ représente votre numéro d'ordinateur.

tap. Lorsqu'on vous demande si vous voulez installer et configurer le service DNS sur cet ordinateur, dites *Oui*.

uisq. Le contrôleur de domaine fonctionnera dans un premier temps en mode mixte.

Vérifiez par *Favoris réseau* que tout est fonctionnel

ATELIER #3

Configuration du client pour les réseaux Microsoft dans un domaine

Equipement

- 1 poste de travail sur Windows 2000 Server en domaine (avec carte réseau)
- 1 poste de travail sur Windows 98 (avec carte réseau)
- 1 poste de travail sur Windows NT 4 Workstation (avec carte réseau)
- 1 poste de travail sur Windows 2000 Professionnal (avec carte réseau)

Objectifs

- Configuration du client pour les réseaux Microsoft sur Windows 98
- Configuration du client pour les réseaux Microsoft sur Windows NT 4 Workstation
- Configuration du client pour les réseaux Microsoft sur Windows 2000 Professionnal

Références à consulter

- http://www.microsoft.com/canada/french/windows2000/
- http://www.microsoft.com/france/technet/produits/win2000s/
- http://www.ntfaqfr.com/install.htm
- http://www.ntfaqfr.com/domaines.html
- http://www.gmg.ch/zoomout/Windows2000/1560/default.htm

Note : Nous assumons que le nom DNS du domaine est cegep-Y.edu (où Y est le numéro d'équipe), et que le nom de domaine NetBIOS est CEGEP-Y (où Y est le numéro d'équipe)

1ière étape : Préparation du poste de travail Windows 98

- Installer les pilotes de la carte réseau.
- Ajouter le **client pour les réseaux Microsoft** dans **Démarrer/ Paramètres/ Panneau de configuration/ Réseau**.

2ième étape : Configuration du client sur Windows 98

2.1

- Allez dans **Démarrer/ Paramètres/ Panneau de configuration/ Réseau**.
- Allez sur l'onglet **Configuration**.
- Sélectionnez **Client pour les réseaux Microsoft** dans la **liste des composants** et cliquez sur **Propriétés**.
- Cochez la case **Ouvrir une session sur un domaine Windows NT**.
- Tapez **CEGEP-Y** (où Y est le numéro de l'équipe) pour le **Domaine Windows NT** et cliquez **OK**.

2.2

- Toujours dans **Démarrer/ Paramètres/ Panneau de configuration/ Réseau**.
- Allez sur l'onglet **Identification**.
- Tapez **CEGEP-Y** (où Y est le numéro de l'équipe) pour le **groupe de travail**.

2.3

- Toujours dans **Démarrer/ Paramètres/ Panneau de configuration/ Réseau**.
- Allez sur l'onglet **Configuration**.
- Sélectionnez **Client pour les réseaux Microsoft** pour l'**ouverture de session réseau principale** et cliquez **OK**.
- Cliquez **Oui** pour **redémarrer maintenant**.

3ième étape : Ouverture de session sur le domaine avec Windows 98

- Avec Windows 98, ouvrez une session sur le domaine CEGEP-Y (où Y est le numéro d'équipe) comme Administrateur.

4ième étape : Préparation de Windows NT 4 Workstation

- Installer les pilotes de la carte réseau.

5ième étape : Configuration du client sur Windows NT 4 Workstation

- Allez dans **Démarrer/ Paramètres/ Panneau de configuration/ Réseau**
- Allez sur l'onglet **Identification**.
- Cliquez sur le bouton **Modifier…**
- Sélectionnez **Membre d'un domaine** et indiquez **CEGEP-Y** (où Y est le numéro d'équipe)
- Cochez la case **Créer un compte d'ordinateur dans le domaine**.
- Spécifiez **Administrateur** comme **Nom d'utilisateur** et spécifiez le **mot de passe**.
- Cliquez **OK**.
- Dans la fenêtre **Réseau**, cliquez sur **Fermer**.
- Cliquez **Oui** pour **Redémarrer maintenant**.

6ième étape : Ouverture de session sur le domaine avec Windows NT 4 Workstation

- Avec Windows NT 4 Workstation, ouvrez une session sur le CEGEP-Y (où Y est le numéro d'équipe) comme Administrateur.

7ième étape : Préparation de Windows 2000 Professionnal

- Installer les pilotes de la carte réseau.

8ième étape : Configuration du client sur Windows 2000 Professionnal

- Allez dans **Démarrer/ Paramètres/ Panneau de configuration/ Système**.
- Allez sur l'onglet **Identification réseau**.
- Cliquez sur **Propriétés**.
- Sélectionnez **Membre d'un domaine** et indiquez **CEGEP-Y** (où Y est le numéro d'équipe).
- Spécifiez **Administrateur** pour le **nom d'utilisateur** et spécifiez le **mot de passe**.
- Cliquez **OK**.
- Cliquez **Oui** pour **Redémarrer maintenant**.

9ième étape : Ouverture de session sur le domaine avec Windows 2000 Professionnal

- Avec Windows 2000 Professionnal, ouvrez une session sur le CEGEP-Y (où Y est le numéro d'équipe) comme Administrateur.

ATELIER #4

Installation Windows 2000 Serveur
2ème partie : Configuration initiale

Préalable à la configuration initiale

Avant de configurer un serveur Windows 2000, il faut avoir planifié certains éléments essentiels au bon fonctionnement. Vous devez avoir planifié :

- Les espaces de noms ('namespace') qui comprennent entre autres choses :
  - Le nom du domaine
  - Le nom DNS du domaine
  - Le nom NETBIOS
- Le nom de l'ordinateur sur lequel est installé Windows 2000 serveur
- Le compte de l'administrateur réseau
- Si le serveur doit être contrôleur de domaine ou non
- Si les serveurs DHCP et DNS résideront sur le serveur ou un autre

Etapes de la configuration initiale

. **Configuration du matériel**

a. Vérifiez la configuration des périphériques installés à l'aide du gestionnaire de périphériques
   i. Y a-t-il des conflits?
   ii. Quels sont les périphériques installés par défaut?
   iii. Modifier la configuration d'un périphérique à l'aide de l'assistant Ajout/Suppression de matériel

. **Configuration des options réseau**

a. Changer le nom de votre serveur pour : **SERVETUxx** (où xx sera donné par votre professeur)
b. Vérifier l'appartenance au domaine **LABO109**
c. Vérifier les noms DNS et NETBIOS de votre ordinateur pour **SERVETUxx**

. **Configuration des composants réseau**

a. Obtenez les informations suivantes de votre configuration réseau à partir des propriétés de Connexion réseau et accès à distance
   i. Nom de la carte réseau (NIC) installée et reliée au rése au
   ii. Nom des services installés
   iii. Nom des protocoles installés
b. Installez/configurez TCP/IP avec les paramètres suivants :
   i. Obtenir une adresse IP automatiquement
   ii. Vérifiez les paramètres de configuration avancés suivants :
      . serveur DNS et serveur WINS

. **Utilisation de la console MMC**

a. Créez une console **MMC** contenant les programmes enfichables ('plug in') suivants :
   - ***Utilisateurs et ordinateurs Active Directory***
   - ***DNS***
   - ***DHCP***

Note : *Vous pouvez démarrer la console MMC à l'aide de la ligne de commande suivante :* ***mmc.exe*** ou encore à partir des programmes du menu : ***Outils d'administration***

. Créez un compte d'usager personnel sur votre serveur

a. A l'aide de l'outil ***Utilisateurs et ordinateurs Active Directory***, configurer votre compte usager **ETUxx**
b. Incorporez le nouveau compte dans le groupe **Administrateurs**
c. Redémarrez l'ordinateur en utilisant le compte **ETUxx**

. Création d'un contrôleur de domaine

a. Créez un contrôleur de domaine supplémentaire pour un domaine existant (**LABO109**) en utilisant la ligne de commande : ***dcpromo.exe***

Variations :

- Créez un sous domaine : **GROUPE01.ATL04** sur un des serveurs
- Changez la localisation des serveurs DNS et DHCP sur deux serveurs différents.
- Vérifiez la reconnaissance de chaque serveur (adresse IP)

ATELIER #5

Les systèmes de fichiers
Windows 2000

Modalité

- Cet atelier doit se faire en équipe de deux.

Equipements

- Une station de travail (Windows 2000 Server, Windows 2000 Professionnel)
- Un accès au réseau

Les systèmes de fichiers

Cet exercice va vous permettre d'utiliser la console *Gestion des disques* que vous avez créée. Celle-ci nous permet de créer de nouvelles partitions et de les modifier.

Etape 1 : Stockage de base

- Réalisez cette étape en tant que Administrateur sous Windows 2000 Server.
  - Ouvrez la console ***Gestion des disques*** à partir d'*Outils d'administration*.
  - Windows 2000 affiche la console *Gestion des disques*.
  - A partir de *Gestion des disques*, identifiez le contenu des disques 0 et 1.
- Disque 0 :
- Disque 1 :
  - Quels sont les types de partition que vous pouvez créer sur le disque 1 ? Expliquez.
  - Créez une partition principale sur le disque 1 ayant les caractéristiques suivantes :

Options	Valeur
Type de partition	Partition principale
Disque sélectionné	Disque 1
Taille de la partition	50 Mo
Lettre de lecteur ou chemin d'accès	H:
Système de fichiers	NTFS
Taille d'unité d'allocation	Par défaut
Nom de volume	VOL1
Formatage rapide	Oui
Activer la compression des fichiers et dossiers	Non

  - Supprimez toutes les partitions du disque 1. Expliquez comment vous avez procédé.
  - Le fait d'avoir supprimé toutes les partitions du disque 1 (interne), amène-t-il un problème pour Windows 2000 Server ? Expliquez.
  - Quels sont les types de partition que vous pouvez créer sur le disque 1 (en stockage de base)? Expliquez.
  - Créez une partition principale ayant les mêmes caractéristiques qu'au point 4.
  - Créez une partition principale ayant les mêmes caractéristiques qu'au point 4, sauf que la lettre sera I: et le nom de volume sera VOL2.
  - Créez une partition étendue de 2Go sur le disque 1.
  - Créez un lecteur logique ayant les caractéristiques suivantes :

Options	Valeur
Type de partition	Lecteur logique
Disque sélectionné	Disque 1
Taille de la partition	25 Mo
Lettre de lecteur ou chemin d'accès	M:
Système de fichiers	NTFS
Taille d'unité d'allocation	Par défaut

Nom de volume	VOL3
Formatage rapide	Oui
Activer la compression des fichiers et dossiers	Non

o. Convertir la partition utilisée par Windows 2000 Server en NTFS.
o. Créez sur le lecteur C: le répertoire ***Montage***.
o. Créez le volume simple ayant les caractéristiques suivantes :

Options	Valeur
Type de volume	Volume simple
Disque sélectionné	Disque 1
Taille du volume	40 Mo
Lettre de lecteur ou chemin d'accès	C:\Montage
Système de fichiers	NTFS
Taille d'unité d'allocation	Par défaut
Nom de volume	Montage
Formatage rapide	Oui

i . Vérification par le professeur.
i . Ouvrez la console ***Gestion Windows 2000 Professionnel*** à partir d'*Outils d'administration*.

- Windows 2000 affiche la console *Gestion Windows 2000 Professionnel*.
-

u. Convertissez le disque 1 (interne) en stockage dynamique.
u. Convertissez la partition utilisée par Windows 2000 Pro en NTFS.
o. Vérification du professeur.

Etape 2 : Stockage dynamique

- Réalisez cette étape en tant que Administrateur sous Windows 2000 Server.

. Ouvrez la console ***Gestion des disques*** à partir d'*Outils d'administration*.

- Windows 2000 affiche la console *Gestion des disques*.

. Convertissez le disque 1 en stockage dynamique. Expliquez la procédure.
. Les partitions LAB1, LAB2 et LAB3 ont été modifiées pour quels types de volume ?
. Quels type de volume pouvez-vous créer sur le disque 1 ? Pourquoi ?
. Créez le volume simple ayant les caractéristiques suivantes :

Options	Valeur
Type de volume	Volume simple
Disque sélectionné	Disque 1
Taille du volume	40 Mo
Lettre de lecteur ou chemin d'accès	N:
Système de fichiers	FAT
Taille d'unité d'allocation	Par défaut
Nom de volume	LAB4
Formatage rapide	Oui

. Convertissez le volume LAB4 en NTFS.
. Vérification du professeur.

Etape 3 : Stockage dynamique (suite)

Réalisez cette étape en tant que Administrateur sur la machine du professeur.

. Ouvrez la console ***Gestion de l'ordinateur*** à partir d'*Outils d'administration*.

Windows 2000 affiche la console *Gestion de l'ordinateur*.

- Convertissez les disques 1 et 2 en stockage dynamique.
- Créez le volume simple ayant les caractéristiques suivantes :

Options	Valeur
Type de volume	Volume simple
Disques sélectionnés	Disque 1
Taille du volume	50 Mo
Lettre de lecteur ou chemin d'accès	I:
Système de fichiers	FAT
Taille d'unité d'allocation	Par défaut
Nom de volume	VOL1
Formatage rapide	Oui

- Copiez des données sur le lecteur I:.
- Créez le volume fractionné ayant les caractéristiques suivantes :

Options	Valeur
Type de volume	Volume fractionné
Disques sélectionnés	Disques 1 et 2
Taille du volume	
Disque 1	40 Mo
Disque 2	60 Mo
Lettre de lecteur ou chemin d'accès	J:
Système de fichiers	FAT
Taille d'unité d'allocation	Par défaut
Nom de volume	VOL2
Formatage rapide	Oui

- Copiez des données sur le lecteur J:.
- Créez le volume en miroir ayant les caractéristiques suivantes :

Options	Valeur
Type de volume	Volume en miroir
Disques sélectionnés	Disques 1 et 2
Taille du volume	
Disque 1	50 Mo
Disque 2	50 Mo
Lettre de lecteur ou chemin d'accès	K:
Système de fichiers	FAT32
Taille d'unité d'allocation	Par défaut
Nom de volume	VOL3
Formatage rapide	Oui

- Copiez des données sur le lecteur K:.
- Créez le volume en miroir ayant les caractéristiques suivantes :

Options	Valeur
Type de volume	Volume en miroir
Disques sélectionnés	Disques 1 et 2
Taille du volume	
Disque 1	40 Mo
Disque 2	40 Mo
Lettre de lecteur ou chemin d'accès	L:
Système de fichiers	FAT
Taille d'unité d'allocation	Par défaut

Nom de volume	VOL4
Formatage rapide	Oui

u. Copiez des données sur le lecteur L:.

u. Créez le volume agrégé par bande ayant les caractéristiques suivantes:

Options	**Valeur**
Type de volume	Volume agrégé par bande
Disques sélectionnés	Disques 1 et 2
Taille du volume	
Disque 1	60 Mo
Disque 2	60 Mo
Lettre de lecteur ou chemin d'accès	M:
Système de fichiers	FAT32
Taille d'unité d'allocation	Par défaut
Nom de volume	VOL5
Formatage rapide	Oui

u. Copiez des données sur le lecteur M:.

u. Créez le volume agrégé par bande ayant les caractéristiques suivantes :

Options	**Valeur**
Type de volume	Volume agrégé par bande
Disques sélectionnés	Disques 0, 1 et 2
Taille du volume	
Disque 0	40 Mo
Disque 1	40 Mo
Disque 2	40 Mo
Lettre de lecteur ou chemin d'accès	N:
Système de fichiers	FAT
Taille d'unité d'allocation	Par défaut
Nom de volume	VOL6
Formatage rapide	Oui

u. Copiez des données sur le lecteur N:.

u. Créez le volume RAID-5 ayant les caractéristiques suivantes :

Options	**Valeur**
Type de volume	Volume RAID-5
Disques sélectionnés	Disques 0, 1 et 2
Taille du volume	
Disque 0	50 Mo
Disque 1	50 Mo
Disque 2	50 Mo
Lettre de lecteur ou chemin d'accès	O:
Système de fichiers	FAT
Taille d'unité d'allocation	Par défaut
Nom de volume	VOL7
Formatage rapide	Oui

u. Copiez des données sur le lecteur O:.

6. Créez le volume RAID-5 ayant les caractéristiques suivantes :

Options	Valeur
Type de volume	Volume RAID-5
Disques sélectionnés	Disques 0, 1 et 2
Taille du volume	
Disque 0	40 Mo
Disque 1	40 Mo
Disque 2	40 Mo
Lettre de lecteur ou chemin d'accès	P:
Système de fichiers	NTFS
Taille d'unité d'allocation	Par défaut
Nom de volume	VOL8
Formatage rapide	Oui

u. Copiez des données sur le lecteur P:.
u. Vérification du professeur.
u. Arrêtez votre machine selon la procédure.
u. Retirez le deuxième disque amovible (celui du bas) et formatez-le à l'aide d'une autre machine. Entre temps, poursuivez la procédure.
u. Redémarrez votre machine sous *Administrateur* et ouvrez la console ***Gestion de l'ordinateur*** à partir d'*Outils d'administration*.
u. Quels sont les volumes que vous pouvez récupérer ? Pourquoi ?
u. Eliminez le volume en miroir ayant comme lettre de lecteur K:. Expliquez la procédure. Quel est le résultat obtenu ?
u. Eliminez le volume RAID-5 ayant comme lettre de lecteur N:. Expliquez la procédure. Quel est le résultat obtenu ?
u. Arrêtez votre machine selon la procédure.
u. Insérez le deuxième disque amovible.
u. Redémarrez votre machine sous *Administrateur* et ouvrez la console ***Gestion de l'ordinateur*** à partir d'*Outils d'administration*.
u. Réparez le volume RAID-5 ayant comme lettre de lecteur O:. Expliquez la procédure. Quel est le résultat obtenu ?
u. Réparez le volume en miroir ayant comme lettre de lecteur L:. Expliquez la procédure. Quel est le résultat obtenu ?
u. Vérification du professeur.
u. Supprimez tous les volumes des disques 1 et 2.
u. Supprimez tous les volumes que vous avez ajoutés du disque 0. (Ne pas supprimer le volume contenant Windows 2000 Server.)
u. Convertissez les disques 1 et 2 en stockage de base.

Vérification du formateur.

ATELIER #6

Les systèmes de fichiers et points de montage
Linux

Modalité

Cet aelier doit se faire de façon individuelle.

Equipements

Une station de travail (Linux Mandrake 9.0)

Les partitions sous linux

Cet exercice va vous permettre de visualiser, de créer et de modifier les partitions d'un disque.

Etape 1 : L'utilitaire cfdisk

Indiquez les informations du disque interne

Device	Boot	Start	End	Blocks	Id	System

Supprimez toute les partitions du disque interne. Quel est la procédure ?

Créez les différentes partitions selon le tableau

Partition	Taille	Système	Numéro du système de fichier	Nom du périphérique
Principale	500 Mo	EXT2		
Lecteur logique	1024 Mo	NTFS		
Lecteur logique	2048 Mo	FAT		
Principale	1024 Mo	EXT3		
Lecteur logique	500 Mo	NetWare		
Lecteur logique	500 Mo	L'un de votre choix mais différent		

Indiquez les informations du disque interne

Device	Boot	Start	End	Blocks	Id	System

Vérification du formateur.

Etape 2 : La commande mount et umount

Montez chacune des partitions réalisées sur le disque interne.

Partition	Device	Commande utilisée
#1		
#2		
#3		
#4		
#5		
#6		

Vérification du formateur.

Démontez chacune des partitions réalisées sur le disque interne.

Partition	Device	Commande utilisée
#1		

#2
#3
#4
#5
#6

Etape 3 : Le fichier fstab

Ouvrez le fichier fstab et indiquez son contenu.

Contenu du fichier

Quelle est la signification de supermount ?

Ouvrez le fichier fstab et ajoutez les lignes nécessaires afin de monter au démarrage les partitions que vous avez créées sur le disque interne.

Partition	Contenu du fichier pour chacune des partitions
#1	
#2	
#3	
#4	
#5	
#6	

Vérification du formeteur.

ATELIER #7

Installation d'une carte réseau

Objectif

Démontrer comment installer une carte réseau dans un PC.

Cadre

Une carte réseau permet à l'ordinateur de se connecter à un réseau et de partager de s fichiers ou des ressources avec d'autres ordinateurs. Les cartes réseau sont assez faciles à installer, dans la mesure où l'on suit quelques directives simples. Après avoir installé la carte réseau, vous bénéficierez d'un accès plus rapide au réseau ou à Internet.

Eléments et outils nécessaires

. Un ordinateur exécutant Windows 95
. Un emplacement d'extension PCI ou ISA
. Le CD-ROM de Windows 95
. Une carte réseau PCI ou ISA (carte Ethernet)
. Une disquette ou un CD-ROM avec les pilotes pour la carte réseau
. Un câble de réseau
. Une trousse à outils
. Un tapis et un bracelet antistatique

Fiche de travail

. Mettez l'ordinateur hors tension et débranchez le cordon d'alimentation. Utilisez un tapis et un bracelet antistatique pour vous mettre à la terre.

e. Retirez du boîtier de l'ordinateur la plaque recouvrant l'emplacement d'extension PCI ou ISA libre dans lequel vous désirez installer la carte réseau.

e. Retirez la carte réseau du sac antistatique. Tenez les coins supérieurs de la carte réseau avec les deux mains. Alignez les pattes de la carte réseau sur l'emplacement et « balancez » doucement la carte d'avant en arrière pour l'insérer dans l'emplacement d'extension. Enfin, fixez la carte au boîtier à l'aide d'une vis.

e. Redémarrez l'ordinateur. Windows 95 déterminera automatiquement le pilote nécessaire pour votre carte réseau. Il pourrait vous demander d'entrer le nom de l'ordinateur et celui du groupe de travail. Choisissez un nom pour votre ordinateur et entrez le nom de groupe de travail que vous a attribué le moniteur de laboratoire.

e. Cliquez deux fois sur l'icône VOISINAGE RESEAU du bureau. Si vous apercevez les noms d'autres ordinateurs dans la fenêtre, cela signifie que la carte réseau fonctionne correctement. Si vous n'apercevez le nom d'aucun autre ordinateur, il est possible que Windows 95 ait installé un mauvais pilote pour votre carte réseau. Dans ce cas, suivez la procédure pour ajouter un pilote :

a. Cliquez sur le bouton DEMARRER, sélectionnez PARAMETRES, puis PANNEAU DE CONFIGURATION.
b. Cliquez deux fois sur l'icône RESEAU. La boîte de dialogue Réseau s'affiche.
c. Cliquez sur le bouton AJOUTER. Sélectionnez CARTE et cliquez de nouveau sur le bouton AJOUTER.
d. Cliquez sur le bouton DISQUETTE FOURNIE. Insérez la disquette de pilotes de la carte réseau dans le lecteur de disquettes. Cliquez sur OK. Le programme d'installation de Windows 95 installe ensuite le pilote.
e. Windows 95 pourrait vous demander de redémarrer l'ordinateur. Après le redémarrage, suivez les instructions données au début de cet exercice pour vérifier si votre carte réseau fonctionne correctement.

Réflexion

Notez dans votre journal les étapes effectuées pour installer une carte réseau. Notez également les précautions que vous avez prises et précisez leur importance.

Réponse :

Assurez-vous que les étudiants consignent dans leur journal les précautions à prendre lorsqu'ils travaillent à l'intérieur d'un ordinateur (ex. : précautions antistatiques, changement d'une chose à la fois, mise hors tension, utilisation des outils appropriés).

ATELIER #8

Installation de câblage structuré

Modalité

- Cet atelier devra se faire en équipe de deux. Il ne fera pas l'objet d'un rapport de laboratoire. Il fera cependant l'objet d'une évaluation sommation (qui compte pour des points) basée sur vos réalisations pratiques.
- Durée 3 heures

Equipements

- Deux stations de travail équipées d'une carte réseau.
- Pince à sertir
- Connecteur RJ45 pour UTP solide
- Bouts de câbles RJ45
- Un testeur de câble (fluke 620)
- Un panneau de raccordement
- Prise murale

Objectifs

- Visualiser les composantes requises pour le câblage d'un réseau local ;
- Fournir une expérience pratique d'installation de câblage ;
- Connecter deux postes de travail en réseau en simulant les différents lieux physiques de connexion ;
- Eexpérimenter l'installation des connecteurs RJ45 les plus utilisées (« jacks », modules, Bix).

Préparation individuelle

- **Lisez attentivement tout l'énoncé du laboratoire.**
- **Lisez dans CISCO dans le module 1 les chapitres 5 et 8 au complet. (très important)**
- Répondez aux questions dans votre cahi er de laboratoire.

1ière étape : Câblage défini par les Norme 568-A vs Norme 568-B

- Les câbles peuvent répondre au norme T568-A ou T568-B, mais il faut se rappeler que ces normes ne sont pas compatibles.
- On peut aussi travailler avec un câblage universel.

1.1 - Déterminer l'ordre des paires du câble répondant à la norme T568-A

1.2 - Déterminer l'ordre des paires du câble répondant à la norme T568-B

1.3 - Quelle est la norme adoptée par le Collège ?

2ième étape : Choisir les équipements de connexion

- Consulter les pages du catalogue de **PANDUIT OU LE SITE WE B** http://www.panduit.com
- En fonction de la norme de câblage T568-A vous devez choisir les équipements suivants :

2.1 - Category 5 Modular Jack (gris)
No. modèle:
Terme français :

2.2 - Connecteur RJ45 pour câble solide
No. modèle :
Terme anglais :

2.3 - Pour quel type de câbles allez-vous idéalement utiliser ces connecteurs?

2.4 - Connecteur RJ45 pour câble multi-brins
No. modèle :

Terme anglais :

2.5 - Pour quel type de câble allez-vous idéalement utiliser ces connecteurs?

2.6 - Un patch panels
No du modèle :
Terme français :
Autre terme :

2.7 - Un crimping tool
No. modèle :
Terme français :

3ième étape : Fabriquer des câbles réseau (UTP)

- Fabriquer un câble direct répondant à la norme T568-A.
- Inscrivez ci-dessous les difficultés rencontrées ainsi qu'une marche à suivre détaillé pour la fabrication d'un tel câble.
- Tester votre câble
  Faites vérifier par le professeur
  Point de vérification _____ _____

  - Quel pourrait être l'utilité de ce câble dans un réseau local?

- Fabriquer maintenant un câble d'interconnexion (cross-over)
- Inscrivez ci-dessous les difficultés rencontrées ainsi qu'une marche à suivre détaillé pour la fabrication d'un tel câble.
  Faites vérifier par le professeur
  Point de vérification _____

  - Quel pourrait être l'utilité de ce câble dans un réseau local?

4ième étape : Choix d'un emplacement pour un local technique

Vous devez effectuer le câblage informatique de l'école Saint-Nulpart. La première étape de votre travail consiste à déterminer où doivent se situer les locaux techniques. Le directeur informatique vous fournit un plan sommaire des trois édifices de l'école. Le point de présence est indiqué.

L'édifice principal a 20 étages. On y retrouve principalement des salles de cours. C'est dans cet édifice que se situe le point de présence.

L'édifice administratif a 10 étages. On y retrouve les bureaux de la direction et l'équipe de support technique.

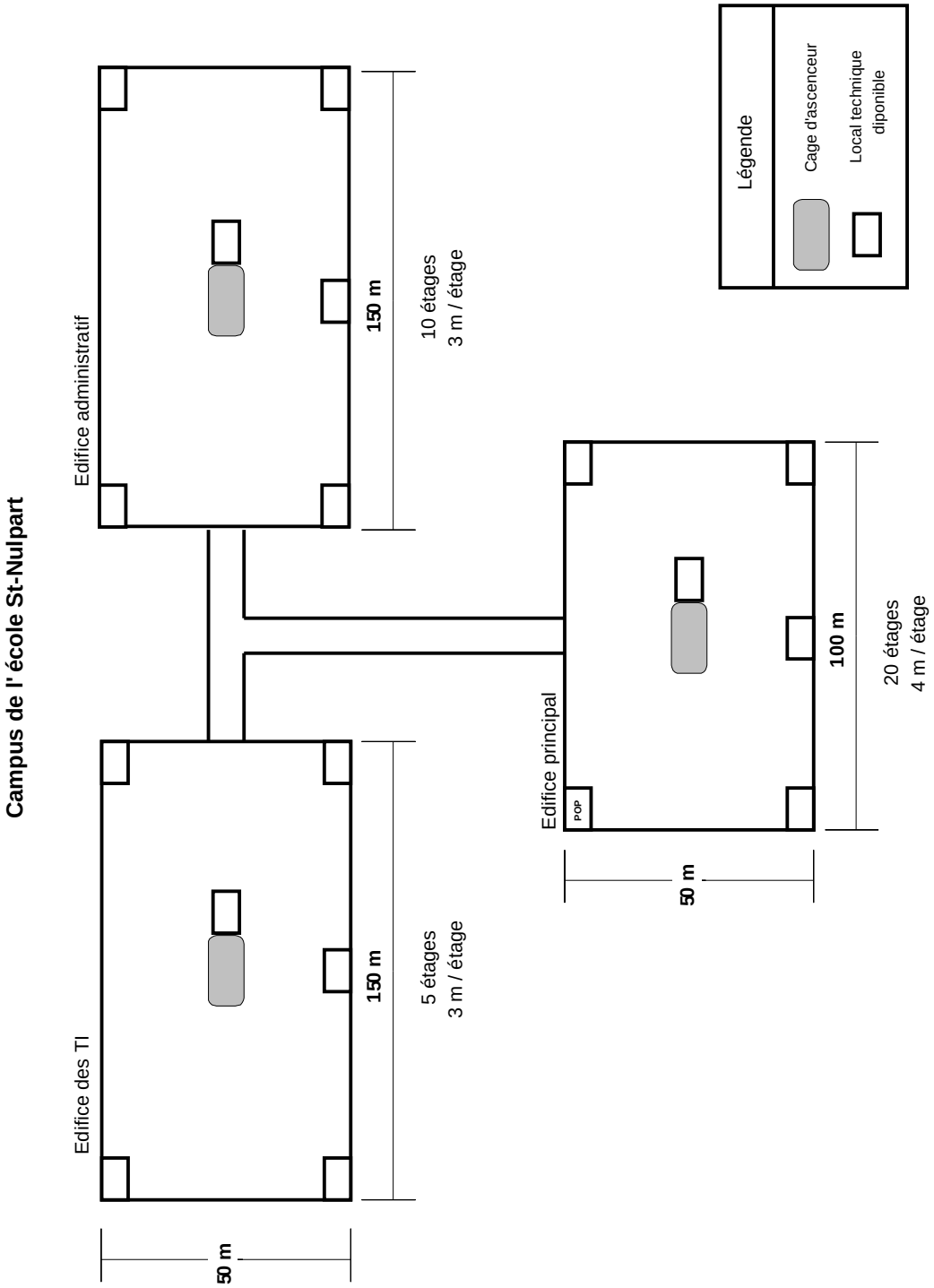
L'édifice des TI a 5 étages. On y retrouve plusieurs laboratoires. Ces locaux sont utilisés principalement pour donner de la formation aux entreprises en technologies de l'information.

Vous devez identifier dans quels locaux, parmi ceux disponibles, seront pl acés le répartiteur principal et les répartiteurs secondaires (MDF et IDF). Vous devez par la suite identifier combien et où seront placés les panneaux de raccordement (MCC, ICC et HCC). Enfin, vous devez identifier le câblage vertical et le câblage horizontal et quel type sera utilisé (fibre, UTP, STP, coaxial).

Acronyme	Anglais	Français
POP	*Point of presence*	Point de présence
MDF	*Main distribution facility*	Répartiteur principal
IDF	*Intermediate distribution facility*	Répartiteur secondaire
MCC	*Main cross connect*	Panneau de raccordement principal
ICC	*Intermediate cross connect*	Panneau de raccordement

		intermédiaire
HCC	*Horizontal cross connect*	Panneau de raccordement horizontal

4.1 - Dessinez le schéma de câblage directement sur le plan ci -dessous. Positionnez quelques machines pour une meilleure vue d'ensemble. Modifiez la légende pour tenir compte du type de câble utilisé.



EVALUATION DE FIN DE MODULE

Instructions préliminaires :

Choisissez 2 machines par étudiant.
Ghoster l'image de Windows 2003 serveur sur l'un des ordinateurs et l'image de Windows XP professionnel sur l'autre. Les noms des images, et la procédure pour le ghost vous ont été donnés en classe. Elles ne seront pas répétée ici.
Veuillez réaliser toutes les taches qui vous sont demandées et répondre aux questions.

Commandes intégrées au système d'exploitation
Dépannage (à quoi sert la commande, à quelle couche elle intervient et quels sont les paramètres de mise en œuvre de cette commande
Quelle est la commande qui permet de vérifier la configuration de TCPIP
Quels sont les paramètres de configuration fournis par cette commande
Si vous obtenez une adresse de type 168.254.100.38 (168.254.x.y) Qu'est ce cela vous donne comme indication au niveau de TCPIP (la machine est configurée pour …. Mais elle n'a pas obtenu …)
Lorsque le masque de sous réseau indiqué par le résultat de la commande est 0.0.0.0 cela indiqe qu'il y a un problème au niveau de l'adresse IP. Quel est ce problème?

Quelle est la commande utilisée pour :
Vérifier que la pile de protocoles TCPIP est bien installée sur la machine locale
Quelles sont les autres pannes que l'on peut vérifier à l'aide de la commande Ping (4 pannes majeures)

Quelles sont les deux commandes utilisées pour diagnostiquer un problème de résolution de nom NetBios

Quelle est la commande utilisée pour diagnostiquer un problème de résolution de nom NetBios avec TCPIP

Lorsque l'on parle de résolution de nom d'hôtes, on fait directement référence au DNS. Quels sont les utilitaires ou commande qui nous permettent de résoudre les problèmes liés à la résolution de noms d'hôtes. Proposez un exemple de panne et une procédure pour le résoudre avec l'utilitaire ou la commande de votre choix

.
vous avez la pannes suivante :

- Depuis un certain temps, le taux d'utilisation de la bande passante est supérieur à 30 % (limite normale pour un réseau typique).
- Vous venez de démarrer la station de travail et aucune requête basée sur TCPIP ne fonctionne. Pourtant vous pouvez joindre tous les serveurs Novell qui utilisent IPX

  - Indiquez comment procéder pour trouver effectuer le diagnostic, la réparer Proposer des solutions (décrire le plus clairement possible la solution adoptée tout en étant concis et bref)
  - Dans le cas où c'est applicable, proposer un outil, un utilitaire, une méthode, ou une technique qui vous permet de diagnostiquer le problème de manière précise.
  - Proposer quelques méthodes de test du câblage en indiquant clairement ce que vous cherchez à mesurer, vérifier ou visualiser et dans quel but.
  - Décrire succinctement au moins trois types d'instruments de mesure pour contrôler le câblage et les problèmes liés aux couches un et deux.

Quel est le moyen que vous pouvez utiliser pour identifier les problèmes enregistrés automatiquem ent par Windows qui se sont produits depuis les dernières 24h
Nom de l'utilitaire qui vous permet d'observer les incidents
Combien d'incident d'erreurs se sont produits au niveau des application, du sytème et de la sécurité

Choisissez en un et expliquer comment le résoudre

analyseurs de protocole
A l'aide d'un analyseur de protocole, veuillez capturer à partir de la carte réseau installée dans votre ordinateur au moins 20000 trames (note il faut installer l'analyseur de protocole le plutôt possible durant l'examen et le laisser capturer des trames pendant au moins 5 à 10 minutes. Certaines versions démo ne permettent pas de capturer plus de 5 minutes de trafic. Mais le plus de trames vous capturez le mieux c'est. De préférence utilisez Protocol Expert de F luke
Répondez au questions suivantes :
Quelle est la durée de la capture?
Combien de trames avez vous saisies?
Nombre de trames de broadcast
Nombre de trames erronées (erreur)
Nombre de trames unicast
A quoi correspond une trame dont la taille est inférieure à 64 b ? quelle est la quantité de trames de ce type trouvées?
A quoi correspond une trame dont la taille est supérieure à 1578 b ? quelle est la quantité de trames de ce type trouvées?
Selon les statistiques de l'analyseur de protocole quelle est la taille de trame qui correspond au plus grand nombre de trames pourquoi
Quel est le % de trames IPX,
Quel est le % de trames ARP,
Veuillez afficher le contenu d'une trame reliée à IP Quel est le numéro de la trame
Quel est le protocole de couche 4
Quel est le protocole application identifié

utilitaires de gestion de réseaux
Installez Optiview console de Fluke
Démarrez la capture de l'analyse des composants réseaux.
Combien de sous réseaux avez vous identifié

Evaluer la charge du trafic réseau

Identifier quoi mesurer et pourquoi, déterminer pour le réseau sous évaluation quelles sont les valeurs de référence par exemple bande passante, %collusion, %erreur, …etc. Quelle est la vitesse de la bande passante

la politique de maintenance préventive
Décrivez au moins dix points importants devant être inclus dans la pol de maint prev.